	<b>Department of Human Services</b> <b>POLICIES AND PROCEDURES</b> <b>MANUAL</b>		Number 8.1.0	Page 1 of 4
	Subject DHS Privacy Policies Introduction		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (**HIPAA**) is a federal law (Public Law 104-191) that focuses on protecting health insurance coverage for workers and their families when they change or lose their jobs (portability), and protecting health information and data integrity, confidentiality, and availability (administrative simplifications/accountability). HIPAA administrative simplification rules are divided into three parts: Transactions and Code Sets; Privacy; and Security. These Hawaii Department of Human Services (DHS) Privacy Policies only address the requirements with respect to the federal Standards for Privacy of Individually Identifiable Health Information Final Rule (HIPAA Privacy Rule) which are found in 45 C.F.R. part 160 and part 164 subparts A and E.

The DHS Privacy Policies are documented in the *DHS Policies and Procedures Manual* Chapter 8, entitled Privacy and Security of Protected Health Information (PHI) that is maintained by the DHS Management Services Office. The following Policies are formally entitled HIPAA Privacy Policies under Chapter 8.1, but will be referred to herein as the DHS Privacy Policies. The DHS Privacy Policies will also be maintained by the HIPAA Privacy Officer and published on the DHS website at: <http://www.state.hi.us/dhs/>.

### 1.0 PURPOSE:

The purpose of the DHS Privacy Policies is to provide requirements applicable to specified DHS divisions and offices to enable them to protect the privacy of individually identifiable health information (hereinafter referred to as protected health information or "PHI"), and to establish the process for developing and implementing specific policies to protect the privacy of PHI.

### 2.0 REFERENCES AND DEFINITIONS:

#### 2.1 REFERENCES

- a. 45 CFR 164.530; and 45 CFR, Parts 160 and 164

#### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A

<b>DHS</b>  <b>P&amp;PM</b>	Subject DHS Privacy Policies Introduction	Number 8.1.0	Page 2 of 4
		Issue/Revision Date April 14, 2003	

### 3.0 POLICY

#### 1. General

HIPAA made significant changes in the protection of PHI that is created, received, transmitted and maintained in any form or medium, by certain divisions and offices of the DHS. Health plans, and health care providers within the DHS that perform specific electronic transactions (e.g., file health care claims electronically), must comply with the HIPAA regulations. The DHS is required to determine the ways in which the HIPAA regulations apply to DHS business practices, and thereby determine its Covered Entity status.

- a. The DHS has designated itself a “Hybrid Entity” which consists of both Covered Components and Non-Covered Components. The DHS, as a Hybrid Entity, is responsible for designating which of its divisions and offices (or portions thereof) are Covered Components and for ensuring that those components comply with HIPAA regulations. Those divisions and offices (or portions thereof) will be referred to hereafter as “Covered Components.” Both the fact that the DHS has determined that it is a Hybrid Entity, and the identity of the Covered Components must be documented. **[See List of Covered Components attached as Appendix B.]** Such documentation must be maintained by the DHS Privacy Officer and be published on the DHS website at: <http://www.state.hi.us/dhs/>.
- b. The DHS must develop policies for its Covered Components to protect the privacy of PHI that is created, received, maintained, or transmitted during its regular course of business. Policies must be reasonably designed to comply with State and Federal Laws, taking into account the scope of the requirement and the nature of activities undertaken that relates to PHI. The HIPAA Privacy Rule will be the primary resource for the DHS Privacy Policies. Each HIPAA Privacy Policy developed by the DHS must apply to all designated Covered Components.

#### 2. Department Policies

- a. The DHS Privacy Officer, and the HIPAA Executive Committee, must develop a systematic approach to policy requirements that will take into account the most efficient and effective methods for ensuring the protection of PHI and equitable Client rights, while promoting consistency in the management of PHI throughout the DHS.
- b. Additions or revisions to the DHS Privacy Policies must be the responsibility of the DHS Privacy Officer.

<b>DHS</b>  <b>P&amp;PM</b>	Subject DHS Privacy Policies Introduction	Number 8.1.0	Page 3 of 4
		Issue/Revision Date April 14, 2003	

- c. The HIPAA Privacy Policies must be amended or revised when applicable provisions of the HIPAA Privacy Rule are amended or revised. All amendments or revisions must be made with the approval of the DHS Privacy Officer.

### **3. Division/Office Responsibilities**

- a. Under applicable Administrative Rules, it is the responsibility of the DHS Covered Components to develop policies/procedures for implementing DHS Privacy Policies at the component (division or staff office) level.
- b. The Covered Components will only use and disclose PHI as provided in their component level policies/procedures. They are also subject to all of the limitations and requirements specified in the DHS Privacy Policies.

### **4. Implementation**

- a. The DHS must ensure compliance with HIPAA privacy requirements through the development and implementation of privacy policies that specify the methods used by the DHS for the protection of PHI. The requirements in these policies must be based on business practices employed by the DHS divisions and offices.
- b. The DHS Privacy Policies include other state and federal requirements that have an impact on the access to, and use and disclosure of, PHI. State laws including those that provide for reporting of disease or injury, child abuse, birth or death and other laws, such as The Uniform Information Practices Act, requiring disclosure of PHI, will remain in effect.
- c. State and Federal Laws that are more stringent than the HIPAA requirements will remain in effect and are not preempted by HIPAA.

### **5. Compliance**

- a. The DHS Covered Components must comply with the privacy policies developed and implemented according to this process by April 14, 2003. This date represents the compliance date specified in the HIPAA Privacy Rule.

#### **4.0 SCOPE**

This policy applies to Covered Components of the DHS as listed in the Appendix B.


<b>DHS</b>  <b>P&amp;PM</b>	Subject DHS Privacy Policies Introduction	Number 8.1.0	Page 4 of 4
		Issue/Revision Date April 14, 2003	

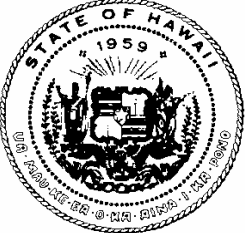
## 5.0 RESPONSIBILITIES

Reserved for future use.

## 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director

	<b>Department of Human Services</b> <b>POLICIES AND PROCEDURES</b> <b>MANUAL</b>		Number Section 8.1.1	Page 1 of 7
	Subject General Privacy		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE:

The intent of this policy is to outline Department of Human Services (DHS) general guidelines and expectations for the necessary collection, use, and disclosure of Protected Health Information (PHI) about Clients in order to provide services and benefits to Clients, while maintaining reasonable safeguards to protect the privacy of their information.

## 2.0 REFERENCES AND DEFINITIONS

### 2.1 REFERENCES


- a. 45 CFR Parts 160.103 and 164.501-530

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A.

## 3.0 POLICY

### 1. General

- a. The DHS will collect, maintain, use, transmit, share and/or disclose information about Clients to the extent needed to administer programs of the DHS Covered Components. 
- b. The DHS must safeguard all confidential information about Clients, inform Clients about DHS' privacy practices and respect Client privacy rights, to the full extent required under this policy.

### 2. Privacy Officer

- a. The DHS must designate a Privacy Officer who is responsible for the development and implementation of the DHS Privacy Policies and Procedures. No DHS Privacy Policy may be amended or revised without the Privacy Officer's approval. The Privacy Officer must assure that the DHS Privacy Policies are amended or revised whenever there is a substantive change in the HIPAA Privacy Rule or other relevant

<b>DHS</b>  <b>P&amp;PM</b>	Subject General Privacy	Number Section 8.1.1	Page 2 of 7
		Issue/Revision Date April 14, 2003	

State or Federal Laws.

- b. The Privacy Officer must monitor compliance with the DHS Privacy Policies and Procedures, and take steps to mitigate any and all known breaches. The Privacy Officer must keep and maintain the DHS Privacy Policies in electronic and hard copy and ensure that they are published on the DHS website.
- c. The Privacy Officer is responsible for keeping documentation with respect to the DHS designation of its Covered Entity status and the identity of its Covered Components, and to ensure that the information is published on the DHS website.
- d. The Privacy Officer is responsible for keeping and maintaining all forms required by or created for the implementation of the DHS Privacy Policies. None of these forms will be modified without approval of the Privacy Officer. **(A list of the forms covered by this section is attached as Appendix C).**

### 3. Training

- a. The DHS must provide training to all DHS Covered Component Staff on the DHS Privacy Policies and Procedures. The DHS must document that all DHS Covered Component Staff have been trained on the DHS Privacy Policies and Procedures.

### 4. Safeguarding information about Clients


- a. DHS Staff and Business Associates must respect and protect the privacy of records and information about Clients who request or receive services from the DHS. This includes, but is not limited to:
  - i. Applicants or recipients of Medicaid assistance;
- b. All information on DHS Clients is confidential and must be safeguarded in accordance with DHS Privacy Policies and Procedures.
- c. The DHS must not use or disclose PHI unless either:
  - i. The Client has authorized the use or disclosure in accordance with DHS Privacy Policy No. 8.1.4, "Uses and Disclosures of Client Information;" or
  - ii. The use or disclosure is specifically permitted under DHS Privacy Policy No. 8.1.4, "Uses and Disclosures of Client Information."

<b>DHS</b>  <b>P&amp;PM</b>	Subject General Privacy	Number Section 8.1.1	Page 3 of 7
		Issue/Revision Date April 14, 2003	

## 5. Conflict with other requirements regarding privacy and safeguarding

- a. In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved, or the meaning of a DHS Privacy Policy is not clear under the circumstances, DHS Staff must not disclose PHI until he/she seeks guidance from supervisors according to established Division or Staff Office Policy and procedures. DHS Staff may also consult with the Privacy Officer.

## 6. DHS Notice of Privacy Practices

- a. DHS Staff must make available a copy of the appropriate, “Notice of Privacy Practices,” to any Client enrolling in or receiving services from DHS Covered Components, describing the actions a Client may take, or request the DHS to take, with regard to the use and/or disclosure their PHI.
- b. The DHS and the DHS Covered Components must provide a  ce that is written in plain language and that contains the following elements:
  - i. The following header:
  - ii. “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”
  - iii. A description, including at least one example, of the types of uses and disclosures that the DHS Covered Components are permitted to make for each of the following purposes: Treatment, Payment, and Health Care Operations;
  - iv. A description of each of the other purposes for which the Covered Entity is permitted or required to use or disclose PHI without the Client’s written authorization;
    - A. The description must include sufficient detail to place the Client on notice of the uses and disclosures that are permitted or required;
  - v. A statement that other uses and disclosures may be made only with the Client’s written authorization and that the Client may revoke such authorization;
  - vi. Information concerning more stringent laws;
  - vii. Information concerning Client contact for the purpose of providing

<b>DHS</b>  <b>P&amp;PM</b>	Subject General Privacy	Number Section 8.1.1	Page 4 of 7
		Issue/Revision Date April 14, 2003	

appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the Client;

- viii. An explanation of how the Client can exercise his/her rights.
- ix. A statement of the following Client rights:
  - A. The right to request restrictions on certain uses and disclosures of PHI
  - B. The right to receive confidential communications of PHI
  - C. The right to inspect and copy PHI
  - D. The right to amend PHI
  - E. The right to receive an accounting of disclosures of PHI
- x. The following information concerning the duties of the DHS:
  - A. The DHS is required by law to maintain the privacy of PHI and to provide Clients with notice of its legal duties and privacy practices with respect to PHI;
  - B. The DHS is required to abide by the terms of the notice currently in effect; and
  - C. The DHS reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains.
  - D. A statement describing the manner in which the DHS will provide Clients with a revised notice.
- xi. A statement that Clients may complain to the DHS and to the United States Department of Health and Human Services (DHHS) if they believe their privacy rights have been violated;
- xii. A brief description of how the Client may file a complaint with the DHS;
- xiii. A statement that the Client will not be retaliated against for filing a complaint;
- xiv. The name, title and telephone number of the DHS contact person or office responsible for handling complaints from Clients;
- xv. The date the Notice was produced;



<b>DHS</b>  <b>P&amp;PM</b>	Subject General Privacy	Number Section 8.1.1	Page 5 of 7
		Issue/Revision Date April 14, 2003	

- xvi. Instances in which more stringent limitations on use and disclosure of PHI may be included in the Notice;
- c. The Notice must not include a limitation affecting the right of the DHS to use or disclose PHI in any way other than required by law.
- d. Nothing in this policy shall prevent the DHS from changing its policies or the “Notice of Privacy Practices” at any time, provided that the changes in the policies or Notice comply with State or Federal Law.
- e. The DHS must promptly revise and distribute its notice whenever changes are made to policies concerning PHI uses or disclosures, Client rights, the DHS legal duties or other privacy practices stated in the notice.
- f. DHS will retain copies of the notices created.
- g. The DHS must notify Clients of the availability of the Notice and how to obtain the Notice no less frequently than once every three years.

## 7. Specific policies to be contained in the DHS Privacy Policies


### a. Business Associate Relationships

The DHS may disclose PHI to Business Associates with whom there is a written contract or Memorandum of Understanding (MOU) as outlined in DHS Privacy Policy No. 8.1.2, “DHS Business Associate Relationships.”

### b. Client Privacy Rights

The DHS must outline the Client’s right to access his/her own PHI, with some exception. This policy also describes specific actions that a Client can take to request restrictions or amendments to their PHI, and the method for filing complaints. These specific actions are outlined in DHS Privacy Policy 8.1.3, “Client Privacy Rights.”


### c. Use and Disclosures of Client Information

The DHS must not use or disclose any information about a Client of DHS Covered Components without a signed authorization for release of that information from the Client, or the Client's legal representative, *unless* authorized by this policy, or as otherwise allowed or required by State or Federal Law, as outlined in DHS Privacy Policy No. 8.1.4, “Uses and Disclosures of Client Information.” DHS Staff must track certain uses and disclosures as described in this policy. DHS Staff must also verify the identity of the person requesting a disclosure 

### d. Use and Disclosures for Research Purposes and Waivers

The DHS may use or disclose a Client's PHI for research purposes as outlined in DHS

<b>DHS</b>  <b>P&amp;PM</b>	Subject General Privacy	Number Section 8.1.1	Page 6 of 7
		Issue/Revision Date April 14, 2003	

Privacy Policy No. 8.1.5, “Uses and Disclosures for Research Purposes.” This policy specifies requirements for using or disclosing PHI with and without a Client's authorization  Research, Health Care Operations and Health Oversight.

**e. Minimum Necessary Information**

The DHS must use or disclose only the minimum amount of information necessary to provide services and benefits to Clients, and only to the extent provided in DHS Privacy Policies and Procedures. When using or disclosing a Client’s PHI, or when requesting a Client’s PHI from a provider or health plan, DHS Staff must make reasonable efforts to limit the amount of information to the Minimum Necessary needed to accomplish the intended purpose of the use, disclosure, or request, as outlined in DHS Privacy Policy No. 8.1.6, “Minimum Necessary Information.”

**f. De-Identification of Client Information and Use of Limited Data Sets**

DHS Staff must follow standards under which Client PHI can be used and disclosed if information that can identify a person has been removed or restricted to a limited data set. Unless otherwise restricted or prohibited by other State or Federal Law, the DHS can use and share PHI as appropriate for the work of the DHS, without further restriction, if the DHS or another entity has taken steps to de-identify the information as outlined in DHS Privacy Policy No. 8.1.7, “De-identification of Client information and Use of Limited Data Sets.”

**g. Administrative, Technical and Physical Safeguards**

DHS Staff must take reasonable steps to safeguard PHI from any intentional or unintentional use or disclosure, as outlined in DHS Privacy Policy No. 8.1.8, “Administrative, Technical, and Physical Safeguards.”

**h. Enforcement, Sanctions and Penalties for Violations of Client Privacy**

The DHS must develop policies that specify appropriate sanctions against DHS Staff who fail to comply with the DHS Privacy Policies. Sanctions may be appropriate to the nature of the violation. Such sanctions may not apply to whistleblower activities, nor to complaints or investigations. These policies are outlined in DHS Privacy Policy No. 8.1.9, “Enforcement, Sanctions, and Penalties for Violations of Client Privacy.”

#### **4.0 SCOPE**

This policy applies to Covered Components of the DHS as listed in the Appendix B.

<b>DHS</b>  <b>P&amp;PM</b>	Subject General Privacy	Number Section 8.1.1	Page 7 of 7
		Issue/Revision Date April 14, 2003	


## 5.0 RESPONSIBILITIES

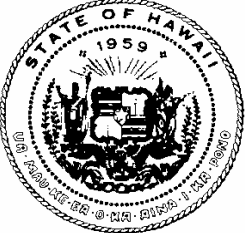
Reserved for future use.

## 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:

  
for Lillian B. Koller, Director

	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.1.2	Page 1 of 5
	Subject Business Associate Relationships		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE:

The HIPAA Privacy rules identify a new category of business relationship, called a “Business Associate.” The purpose of this policy is to specify when the Department of Human Services (DHS) may disclose a Client’s Protected Health Information (PHI) to a Business Associate of the DHS, and to specify provisions that must be included in DHS contracts with Business Associates.

## 2.0 REFERENCES AND DEFINITIONS

### 2.1 REFERENCES

- a. 45 CFR 160.103, 164.502, 164.504, 164.530 and 164.532

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A.

## 3.0 POLICY

### 1. General

- a. This policy only applies to contractors or business partners that come within the definition of a “Business Associate.” (See, Glossary of Terms, Appendix A) The DHS has many contractual and business relationships, and the DHS has policies related to its contracts and business relationships. However, not all contractors or business partners are “Business Associates” of the DHS.
- b. If a contractor or business partner is a “Business Associate,” those contracts that define the contractual relationship remain subject to all State and Federal Laws and policies governing the contractual relationship. A “Business Associate” relationship also requires additional contract provisions. The additional contract requirements are described below.
- c. The DHS must identify and document its Business Associates.

### 2. Business Associate Relationship

- a. A Business Associate relationship is formed only if PHI is to be used, created, or disclosed in the relationship.
- b. The following are **not** Business Associates or Business Associate relationships:
  - i. DHS Staff, offices, and programs;
  - ii. Medical providers providing treatment to Clients;

<b>DHS</b>  <b>P&amp;PM</b>	Subject Business Associate Relationships	Number 8.1.2	Page 2 of 5
		Issue/Revision Date April 14, 2003	

- iii. Eligibility determinations involving DHS Clients, between government agencies;
- iv. Payment relationships, such as when the DHS is paying medical providers, managed care organizations, or other entities for services to DHS Clients, when the entity is providing its own normal services that are not on behalf of the DHS;
- v. When a Client's PHI is disclosed based solely on a Client's authorization;
- vi. When a Client's PHI is not being disclosed by the DHS or created for the DHS; and
- vii. When the only information being disclosed is information that is de-identified in accordance with DHS Privacy Policy No. 8.1.7, "De-identification of Client Information and Use of Limited Data."

### **3. Disclosure to a Business Associate**

- a. The DHS may disclose a Client's PHI to a Business Associate and may allow a Business Associate to create or receive a Client's PHI on behalf of the DHS, if:
  - i. The DHS first enters into a written contract, or other written agreement or arrangement, with the Business Associate before disclosing a Client's PHI to the Business Associate, in accordance with the requirements of section 4, below, of this policy.
  - ii. The written contract or agreement provides satisfactory assurance to the DHS that the Business Associate will appropriately safeguard the information.
- b. If a Business Associate is required by law to perform a function or activity on behalf of the DHS, or to provide a service to the DHS, the DHS may disclose PHI to the Business Associate to the extent necessary to enable compliance with the legal requirement, without a written contract or agreement, if:
  - i. The DHS attempts in good faith to obtain satisfactory assurances from the Business Associate that the Business Associate will protect PHI to the extent specified in section 4 of this policy; and
  - ii. If such attempt fails, the DHS documents the attempt and the reasons that such assurances cannot be obtained.

### **4. Contract Requirements applicable to Business Associates**

- a. A contract between the DHS and a Business Associate must include terms and conditions that:
  - i. Establish the permitted and required uses and disclosures of PHI by the Business Associate. The contract may not authorize the Business Associate to further use or disclose PHI obtained from the DHS in a manner that would violate the requirements of the HIPAA Privacy Rule if executed by the DHS, except that the contract may permit the Business Associate to:

<b>DHS</b>  <b>P&amp;PM</b>	Subject Business Associate Relationships	Number 8.1.2	Page 3 of 5
		Issue/Revision Date April 14, 2003	

- i. Use and disclose PHI for the proper management and administration of the Business Associate; and
- ii. Collect data related to DHS operations.
- ii. Provide that the Business Associate must:
  - i. Not use or further disclose PHI other than as permitted or required by the contract or as required by law;
  - ii. Use appropriate safeguards to prevent use or disclosure of the information consistent with the requirements of the Business Associate contract;
  - iii. Report to the DHS any use or disclosure not allowed by the contract of which the Business Associate has become aware;
  - iv. Ensure that any agents or subcontractors with whom PHI must be shared agree to the same restrictions and conditions that apply to the Business Associate under the contract;
  - v. Make PHI available to the Client in accordance with the DHS Privacy Policy No. 8.1.3, "Client Privacy Rights;"
  - vi. Make PHI available for amendment and incorporate any amendments in accordance with DHS Privacy Policy No. 8.1.3, "Client Privacy Rights;"
  - vii. Make available the information required to provide an accounting of disclosures in accordance with DHS Privacy Policy No. 8.1.3, "Client Privacy Rights;"
  - viii. Make its internal practices, books, and records relating to the use and disclosure of PHI available to the DHS and to the Department of Health and Human Services (DHHS) for the purpose of determining DHS compliance with federal requirements; and
  - ix. At termination of the contract, if feasible, return or destroy all PHI that the Business Associate still maintains in any form, and keep no copies thereof. If not feasible, the Business Associate must continue to protect the information.
- iii. Authorize termination of the contract if the DHS determines that the Business Associate has violated a material term of the contract.

**5. Business associate relationships between the DHS and another governmental entity**

- a. The DHS may enter into a Memorandum of Understanding (MOU), rather than a contract, with the Business Associate if the Memorandum of Understanding contains terms covering all objectives above, of this policy;
- b. The written contract, agreement, or memorandum is not necessary, if other law or regulations contain requirements applicable to the Business Associate that accomplish the same objective.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Business Associate Relationships	Number 8.1.2	Page 4 of 5
		Issue/Revision Date April 14, 2003	

## **6. Other requirements for written contracts or agreements**

The written contract or agreement between the DHS and the Business Associate may permit the Business Associate to:

- i. Use PHI it receives in its capacity as a Business Associate to the DHS, if necessary:
  - i. For proper management and administration of the Business Associate; or
  - ii. To carry out the legal responsibilities of the Business Associate.
- ii. Disclose PHI it receives in its capacity as a Business Associate if:
  - i. The disclosure is required by law; or
  - ii. The Business Associate receives assurances from the person to whom the PHI is disclosed that:
    - A. It will be held or disclosed further only as required by law or for the purposes for which it was disclosed to such person.
    - B. The person notifies the Business Associate of any known instances in which the confidentiality of the information has been breached.

## **7. Business Associate non-compliance, known breaches and complaints**

- a. If the DHS knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the contract or other arrangement, the DHS must take reasonable steps to cure the breach or end the violation, as applicable.
- b. DHS Staff who receive a Client complaint, or a report or complaint from any source, about inappropriate uses or disclosures of information by Business Associates, must provide information regarding that report or complaint to appropriate Covered Component Administration.
- c. If a Client complaint is made directly to the DHS Privacy Officer, the DHS Privacy Officer must contact the appropriate DHS Covered Component.
- d. The DHS Covered Component must send a letter to the Business Associate requesting that the Business Associate review the circumstances related to the complaint, and document and mitigate (if necessary) any breaches. The DHS Covered Component may require that the Business Associate respond, in writing, within 10 business days to the DHS letter.
- e. If the Covered Component cannot resolve the complaint with the Business Associate, the Covered Component shall share the information with the DHS Privacy Officer.
  - i. If determined necessary and appropriate, the DHS Covered Component's administration, in consultation with the DHS Privacy Officer, will generate a "cure letter" outlining required remediation in order for the Business Associate to attain contract compliance.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Business Associate Relationships	Number 8.1.2	Page 5 of 5
		Issue/Revision Date April 14, 2003	

- f. In cases where contract compliance cannot be attained, the DHS must:
  - i. Terminate the contract, if feasible.
  - ii. If termination is not feasible, the DHS Privacy Officer must report the problem to the DHHS, Office of Civil Rights.

#### 4.0 SCOPE


This policy applies to Covered Components of the DHS as listed in the Appendix B.

#### 5.0 RESPONSIBILITIES

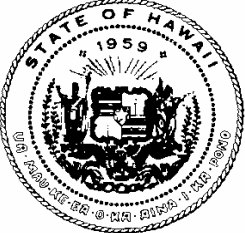
Reserved for future use.

#### 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director



	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.1.3	Page 1 of 14
	Subject Client Privacy Rights		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE

The intent of this policy is to establish the privacy rights that the Department of Human Services (DHS) Clients have regarding the use and disclosure of their Protected Health Information (PHI) that is held by the DHS, and to describe the process for filing a complaint should Clients feel those rights have been violated.

## 2.0 REFERENCES AND DEFINITIONS

### 2.1 REFERENCES

- a) 45 CFR Parts 164.500 – 164.502, 164.520 – 164.530
- b) Hawaii Revised Statutes, Chapter 92F

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A.

## 3.0 POLICY

### 1. General

- a. DHS Clients have the right to, and the DHS will not deny, the following:
  - i. Access to their own PHI contained in their own DHS case files or records, subject to certain limitations;
  - ii. Receive an accounting of disclosures the DHS has made of their PHI for up to six years prior to the date of requesting such accounting. This information will not be available prior to the effective date of this policy (April 14, 2003) and certain limitations do apply as outlined in section 6 of this policy; and
  - iii. Submit complaints if they believe or suspect that information about them has been improperly used or disclosed, or if they have concerns about the privacy policies of the DHS.
- b. Clients may ask the DHS to take specific actions regarding the use and disclosure of their PHI and the DHS may either approve or deny the request consistent with applicable law. Specifically, Clients have the right to request:
  - i. That the DHS restrict uses and disclosures of their PHI while carrying out treatment, payment activities, or health care operations;
  - ii. To receive information from the DHS by alternative means, such as mail, fax or

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 2 of 14
		Issue/Revision Date April 14, 2003	

telephone, or at alternative locations; and

- iii. That the DHS amend the Client's PHI that is held by the DHS.
- c. Clients have a right to receive a Notice of Privacy Practices.
  - i. The DHS Covered Components must use an approved "Notice of Privacy Practices" ("Notice") to inform Clients about how a DHS Covered Component may use and/or disclose their PHI. The Notice also describes the actions a Client may take, or request the DHS to take, with regard to the use and/or disclosure of their PHI.
  - ii. The policies related to the Notice and the distributions of the Notice are addressed in DHS Privacy Policy No. 8.1.1, "General Privacy."
  - iii. Nothing in this policy, or the policy related to the Notice must prevent the DHS from changing its policies or the Notice at any time, provided that the changes in the policies or Notice comply with State or Federal Law.
  - iv. DHS Covered Components will promptly revise and distribute their Notice whenever material changes are made to its policies concerning PHI uses or disclosures, Client rights, the DHS' legal duties or other privacy practices stated in the Notice.
  - v. The DHS and its Covered Components must retain copies of the Notices created.

## **2. Rights of Clients to request restrictions on use and disclosure of their PHI**

- a. Clients have the right to request restrictions on the use and/or disclosure of their PHI, for:
  - i. Carrying out treatment, payment, or health care operations;
  - ii. Disclosure of PHI to a relative or other person who is involved in the Client's care.
- b. The DHS applies confidentiality laws applicable to specific DHS Covered Components or activities to protect the privacy of PHI. Even if those laws would permit the DHS to make a use or disclosure of PHI, a DHS Client has the right to request a restriction on a use or disclosure of that PHI.
- c. All requests may be submitted by completing the appropriate "Request to Restrict Disclosure of Protected Health Information" form.
- d. The DHS must document the Client's request, and the reasons for granting or denying the request in the Client's hard copy or electronic DHS case record file.
  - i. Prior to any disclosure of Client PHI, DHS Staff must confirm that such use or disclosure has not been granted a restriction by reviewing the Client's case file.
- e. If the DHS agrees to a Client's request for restriction, the DHS must not use or disclose PHI that violates the restriction.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 3 of 14
		Issue/Revision Date April 14, 2003	

- f. **The DHS may deny the request or may agree to a restriction more limited than what the Client requested.** A restriction agreed to by the DHS under this section, is not effective to prevent uses or disclosures permitted or required by the DHS Privacy Policy No. 8.1.4, “Uses and Disclosures of Client Information,” sections 3.5 and 3.7, or required by existing State or Federal Law.

**Exception:** Consistent with State or Federal Law, certain programs can only use PHI that is authorized by the Client, such as alcohol and drug programs. For those Clients, the DHS will honor their requests for restriction by making sure that the authorization clearly identifies the authorized recipients of the information.

- g. **Emergency Treatment:** In the event of a circumstance in which the restricted PHI is needed to provide emergency treatment, the DHS may use or disclose such PHI to the extent needed to provide the emergency treatment. However, the provider must be notified of the restriction and once the emergency situation subsides, the DHS must ask the provider not to redisclose the PHI.
- h. **Termination of Restrictions:** Clients have the right to request termination of restrictions they have requested on the use and/or disclosure of their PHI and such requests will be honored if:

- i. The Client agrees to or requests the termination in writing;
- ii. The Client orally agrees to a termination and the oral agreement must be documented as follows:
  - A. The DHS will inform the Client in writing that it is terminating its agreement to a restriction.
  - B. The termination is only effective with respect to PHI created or received after the Client has been informed.

- i. The DHS is not required to agree to a restriction requested by the Client.
  - i. The DHS may not agree to restrict uses or disclosures of PHI if the restriction would adversely affect the quality of the Client’s care or services;
  - ii. The DHS cannot agree to a restriction that would limit or prevent the DHS from making or obtaining payment for services.

**Exception:** For Alcohol and Drug programs, Federal law (42 CFR Part 2) prohibits the DHS from denying Client requests for restrictions on uses and disclosures of their PHI regarding treatment or rehabilitation.

- j. The DHS may terminate its agreement to a restriction if:
- i. The Client agrees to or requests termination of the restriction in writing;
  - ii. The Client orally agrees to, or requests termination of the restriction. The DHS will document the oral agreement or request in the Client’s DHS case record file; or
  - iii. The DHS informs the Client in writing that the DHS is terminating its agreement

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 4 of 14
		Issue/Revision Date April 14, 2003	

to the restriction. Information created or received while the restriction was in effect must remain subject to the restriction.

### **3. Rights of Clients to request to receive PHI from the DHS by alternative means or at alternative locations**

- a. The DHS must accommodate reasonable requests by Clients to receive communications at an alternative location or by alternative means.
  - i. The Client must specify the preferred alternative means or location;
  - ii. Requests for alternative means or alternative locations for PHI may be made orally or in writing;
  - iii. If a Client makes a request orally, the DHS must document the request;
  - iv. If a Client makes a request by telephone or electronically, the DHS must document the request and verify the identity of the requestor in accordance with DHS Privacy Policy No. 8.1.4, " Uses and Disclosures of Client Information";
  - v. Prior to any PHI being sent to the Client, DHS Staff must confirm if the Client has requested an alternate location or by alternate means, and if the DHS has granted that request, by reviewing the Client's case file.
- b. The DHS must accommodate reasonable requests by Clients to receive communications by alternative means, such as by mail, fax or telephone.
- c. The DHS may terminate its agreement to an alternative location or method of communication if:
  - i. The Client agrees to or requests termination of the alternative location or method of communication in writing or orally. The DHS will document the oral agreement or request in the Client's DHS case record file; or
  - ii. The alternative location or method of communication is not effective.

### **4. Rights of Clients to access their PHI**

- a. Clients have the right to access, inspect, and obtain a copy of PHI on their own cases in DHS files or records, consistent with Federal law and the Hawaii Uniform Information Practices Act.
- b. The DHS will assure that Clients may access their PHI that the DHS uses in whole or part to make decisions about them, subject to certain limitations as outlined in this policy.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 5 of 14
		Issue/Revision Date April 14, 2003	

- c. The DHS must arrange with the Client for providing the requested access in a time and place convenient for the Client and the DHS. This may include mailing the PHI to the Client if the Client so requests or agrees. See section 3.3, above.
- d. All requests for access must be made having the Client complete the appropriate "Authorization to Disclose Confidential Information." Form.
- e. **Denial of Access to PHI:** The DHS may deny Clients access to their own PHI if:
  - i. It was obtained from someone other than a health care provider under a promise of confidentiality, and disclosure to the Client would be reasonably likely to reveal the source of the information;
  - ii. It is information compiled for use in ongoing or pending civil, criminal, or administrative proceedings against the Client;
  - iii. It is information subject to the federal Clinical Labs Improvement Amendments of 1988, or exempt pursuant to substance abuse 42 CFR 493.3(a)(2);
  - iv. The DHS believes, in good faith, that the information can cause harm to the Client or to any other person;
  - v. The information is protected by attorney work-product privilege; or
  - vi. The release of the information is prohibited by State or Federal Law.
- f. If the DHS maintains PHI about the Client in a record that includes PHI about other people, the Client is only authorized to see PHI about himself/herself, except as provided below:
  - i. If the other person identified in the file is a minor child of the Client, and the Client is authorized under Hawaii law to have access to the minor's PHI or to act on behalf of the minor for making decisions about the minor's care, the Client may also obtain PHI about the minor.
  - ii. Protection and advocacy groups authorized by law to protect and advocate the rights of Clients with developmental disabilities under part C of the Developmental Disabilities Assistance and Bill of Rights Act (42 U.S.C. 6041 et seq.) and the rights of Clients with mental illness under the Protection and Advocacy for Individuals with Mental Illness Act (42 U.S.C. 10801 et seq.) must have access to all records, in accordance with applicable law.'
- g. Before the DHS denies a Client access to his/her PHI because there is a good faith belief that its disclosure could cause harm to the Client or to another person, the DHS decision to deny must be made by a licensed health care professional or other designated DHS Staff, and the DHS must make a review of this denial available to the Client. If the Client wishes to have this denial reviewed, the review must be done by a designated DHS staff or licensed health care professional who was not involved in the original decision.
- h. If the DHS denies access under this policy, the Client has the right to have the decision reviewed by a licensed health care professional or other designated Staff not

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 6 of 14
		Issue/Revision Date April 14, 2003	

directly involved in making the original denial decision if:

- i. The PHI makes reference to another person, and a licensed health care professional or other designated Staff has determined, in the exercise of professional judgment, that the PHI requested may cause substantial harm to the Client or another person; or
- ii. The request for access is made by the Client's legal representative, and a licensed health care professional or other designated DHS Staff has determined, in the exercise of professional judgment, that allowing the legal representative to access the PHI may cause substantial harm to the Client or to another person.
- iii. The reviewer must determine, within a reasonable time, whether or not to approve or deny the Client's request for access, in accordance with this policy.
- iv. The DHS must then:
  - A. Promptly notify the Client in writing of the reviewer's determination; and
  - B. Take action to carry out the reviewer's determination.
- i. **Written Denial Required:** The Client must be provided with a written denial sent or provided within the time limits specified in this Section below. Containing the following information in plain language:
  - i. The basis for the denial;
  - ii. A statement of the Client's review rights including a description of how the Client may exercise such review rights;
  - iii. A description of how the Client may complain to the DHS and/or the United States Department of Human Services (DHHS) pursuant to the complaint procedures described in section 7 of this policy, including the name or title, and telephone number of the contact person or office designated.
  - iv. Provisions for access to any other requested information, after excluding the PHI to which access is denied;
- j. **PHI Maintained by another Entity:** The DHS must inform the Client of where to direct the request for access if the DHS does not maintain the requested PHI, and knows where such PHI is maintained (such as by a medical provider, insurer, other public agency, private business, or other non-DHS entity).
- k. **Provision of Access to PHI:** The DHS must permit a Client to review the Client's PHI in the Client's case file or record and have a copy made no later than 10 working days after receiving the request.
  - i. The 10 working day period may be extended once for an additional 20 working days if the DHS provides to the Client, within the initial ten working days, a written notice of the delay, an explanation of the unusual circumstances causing the delay, and the date by which the DHS will complete its action on the request;

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 7 of 14
		Issue/Revision Date April 14, 2003	

- l. If the DHS maintains the same PHI in more than one format (such as electronically and in a hard-copy file) or at more than one location, the DHS need only provide the requested PHI once.
- m. **Form of Information:** The DHS must provide the requested PHI in a form or format requested by the Client, if readily producible in that form or format. If not readily producible, the DHS will provide the information in a readable hard-copy format that is reasonably intelligible or such other format as agreed to by the DHS and the Client. The DHS must provide a translation into common terms of any machine readable code or any code or abbreviation employed for internal DHS use.
- n. **Summary of PHI:** The DHS may provide the Client with a summary of the requested PHI, in lieu of providing access, or may provide an explanation of the PHI if access had been provided, if:
  - i. The Client agrees in advance; and
  - ii. The Client agrees in advance to any fees the DHS may impose, per subsection o, below.
- o. **Fees:** If a Client (or legal guardian or representative) requests a copy of the requested PHI, or a written summary or explanation, then the DHS may impose a reasonable, cost-based fee, limited to covering the following:
  - i. Copying the requested PHI, including the costs of supplies and of the labor of copying;
  - ii. Postage, when the Client has requested or agreed to having the information mailed; and
  - iii. Preparing an explanation or summary of the requested PHI, if agreed to in advance by the Client;
- p. The DHS must give the Client access to any other requested information, after excluding the information to which access is denied.

## 5. Rights of Clients to request amendments to their PHI

- a. Clients have the right to request that the DHS correct or amend their PHI in the DHS files.
- b. All requests for amendments must be executed by having the Client complete the appropriate "Request to Amend Confidential Information" form.
- c. The DHS must honor requests for alternative methods of making this request if reasonable accommodations are needed.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 8 of 14
		Issue/Revision Date April 14, 2003	

- d. Prior to any decision, based on a Client's request for the DHS to amend PHI in a designated record set, the person or office designated by a DHS Covered Component for this purpose must review the request and any related documentation. The designated person may be a DHS Staff person involved in the Client's case.
- e. Requests to amend any other information that is not PHI must be processed pursuant the DHS policies and procedures relating to request to amend personal records under the Uniform Information Practices Act.
- f. The DHS is not obligated to agree to an amendment and may deny the requests or limit its agreement to amend. The DHS may deny (or limit) the Client's request for amendment if:
  - i. The DHS finds the PHI to be accurate and complete;
  - ii. The PHI was not created by the DHS, unless the Client provides a reasonable basis to believe that the originator of such information is no longer available to act on the requested amendment;
  - iii. The PHI is not part of the DHS records; or
  - iv. The PHI would not be available for inspection or access by the Client, pursuant to this policy.
- g. The DHS must act on a Client's request for amendment within 20 business days of receipt as follows:
  - i. If the DHS grants the request, in whole or in part, the DHS must:
    - A. Make the appropriate amendment to the PHI or records, and document the amendment in the Client file or record;
    - B. Notify the Client that the amendment has been accepted;
    - C. Seek the Client's agreement to notify other relevant persons or entities, with whom the DHS has shared or needs to share the amended PHI, of the amendment; and
    - D. Make reasonable efforts to inform, and to provide the amendment within a reasonable time to:
      - I. Persons named by the Client as having received PHI and who thus need the amendment; and
      - II. Persons, including Business Associates of the DHS, that the DHS knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on the PHI to the Client's detriment.
  - ii. If an amendment is denied, in whole or in part, the DHS must make a written final determination on its denial of the amendment within 30 business days after the request for review was received; and
  - iii. The DHS must inform the Client in writing of its denial, the reason for the denial,



<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 9 of 14
		Issue/Revision Date April 14, 2003	

and the DHS procedures for review. The denial must:

- A. Be sent or provided within the time limits specified above;
- B. State the basis for the denial, in plain language;
- C. Explain the Client's right to submit a written statement disagreeing with the denial and how to file such a statement. If the Client does so:
  - I. The DHS will enter the written statement into the Client's DHS case file;
  - II. The DHS may also enter a DHS written rebuttal of the Client's written statement into the Client's DHS case record. The DHS must send or provide a copy of any such written rebuttal to the Client;
  - III. The DHS must include a copy of that statement, and of the written rebuttal by the DHS if any, with any future disclosures of the relevant information; and
  - IV. Explain that if the Client does not submit a written statement of disagreement, the Client may ask that if the DHS makes any future disclosures of the relevant information, the DHS must also include a copy of the Client's original request for amendment and a copy of the DHS written denial; and
  - V. Inform the Client of the applicable procedures for obtaining appropriate judicial remedy;
- D. Provide information on how the Client may file a complaint with the DHS, or with the DHHS, Office of Civil Rights, subject to section 7 of this policy.
- h. The DHS may provide rebuttal to a statement of disagreement concerning the denial from the Client by providing the Client with a copy of a rebuttal to a statement of disagreement.
- i. Upon receipt of notice of correction and amendment to a Client record from an outside source, the DHS will document receipt of the notice and the correction or amendment contained in the notice in the Client record.

## **6. Rights of Clients to an accounting of disclosures of PHI**

- a. Clients have the right to receive an accounting of disclosures of PHI that the DHS has made for any period of time, not to exceed six years, preceding the date of the request for the accounting, but it does not apply to disclosures made prior to the effective date of this policy, April 14, 2003.
- b. The accounting will only include PHI not previously authorized by the Client for use or disclosure, and will not include PHI collected, used or disclosed for treatment, payment or health care operations for that Client.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 10 of 14
		Issue/Revision Date April 14, 2003	

- c. All requests for an accounting of disclosures must be executed by having the Client complete a “Request for Accounting of Disclosures of Health Information” form.
- d. When a Client requests an accounting of disclosures that the DHS has made of their PHI, the DHS must provide that Client with a written accounting of such disclosures made during the six- year period (or lesser time period if specified by the requesting Client) preceding the date of the Client’s request.
- e. An accounting of disclosures provided to a requestor must include for each disclosure:
  - i. Date of the disclosure;
  - ii. Name of the entity or person who received the PHI and, if known, the address of such entity or person;
  - iii. A brief description of the PHI disclosed that reasonably informs the Client of the basis for the disclosure, or, in lieu of such statement, a copy of the Client’s written request for a disclosure, if any;
  - iv. A brief statement of the purpose of the disclosure.
- f. **Disclosures that are not required to be tracked and accounted for** are those that are:
  - i. Authorized by the Client;
  - ii. Made prior to April 14, 2003;
  - iii. Made to carry out Treatment, Payment, and Health Care Operations;
  - iv. Made to the Client;
  - v. Made to persons involved in the Client’s health care, as provided in the DHS Privacy Policy No. 8.1.4 “Uses and Disclosures of Client Information” section 3.9.b.
  - vi. Made as part of a limited data set in accordance with the DHS Privacy Policy No. 8.1.7, “De-identification of Client Information and Use of Limited Data Sets.”
  - vii. For national security or intelligence purposes; or
  - viii. Made to correctional institutions or law enforcement officials having lawful custody of an inmate if disclosure is necessary to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual PHI about such inmate or individual, if the correctional institution or such law enforcement official represents that such PHI is necessary for:
    - A. The provision of health care to such individuals;
    - B. The health and safety of such individual or other inmates;
    - C. The health and safety of the officers or employees of or others at the correctional institution;

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 11 of 14
		Issue/Revision Date April 14, 2003	

- D. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
- E. Law enforcement on the premises of the correctional institution; and
- F. The administration and maintenance of the safety, security, and good order of the correctional institution.

**Note:** An individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

- g. **Disclosures to be Included in an Accounting:** Examples of disclosures of PHI that are required to be listed in an accounting (assuming that the disclosure is permitted by other confidentiality laws applicable to the Client's PHI and the purpose for which it was collected or maintained) include:
  - i. Abuse Report: PHI about a Client provided by DHS Staff (other than protective services staff who respond to such report) pursuant to mandatory abuse reporting laws to an entity authorized by law to receive the abuse report.
  - ii. Audit Review: PHI provided by DHS Staff from a Client's record in relation to an audit or review (whether financial or quality of care or other audit or review) of a provider or contractor.
  - iii. Health and Safety: PHI about a Client provided by DHS Staff to avert a serious threat to health or safety of a person.
  - iv. Health Oversight: PHI provided to a Health Oversight Agency for activities necessary for the appropriate oversight of the health care system; government benefit programs for which health information is relevant to beneficiary eligibility; entities subject to government regulatory programs for which health information is necessary for determining program standards; or entities subject to civil rights laws for which health information is necessary for determining compliance.
  - v. Licensee/Provider: PHI provided by the DHS from a Client's records in relation to licensing or regulation or certification of a provider or licensee or entity involved in the care or services of the Client.
  - vi. Legal Proceeding: PHI about a Client that is ordered to be disclosed pursuant to a court order in a court case, administrative hearing or other legal proceeding – include a copy of the court order with the accounting.
  - vii. Law Enforcement Official/Court Order: PHI about a Client provided to a law enforcement official pursuant to a court order – include a copy of the court order with the accounting.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 12 of 14
		Issue/Revision Date April 14, 2003	

- viii. Law Enforcement Official/Deceased: PHI provided to law enforcement officials or medical examiner about a person who has died for the purpose of identifying the deceased person, determining cause of death, or as otherwise authorized by law.
- ix. Law Enforcement Official/Warrant: PHI provided to law enforcement official in relation to a fleeing felon or for whom a warrant for their arrest has been issued and the law enforcement official has made proper request for the PHI, to the extent otherwise permitted by law.
- x. Public Health Official: PHI about a Client provided by DHS Staff (other than staff employed for public health functions) to a public health official, such as the reporting of disease, injury, or the conduct of a public health study or investigation information and the purpose for which it was collected or maintained) include:
- xi. Public Record: PHI about a Client that is disclosed pursuant to a Public Record request without the Client's authorization.
- h. **Multiple Disclosures to Same Requestor**: If, during the time period covered by the accounting, the DHS has made multiple disclosures of PHI to the DHHS for determining the DHS' compliance with the Privacy Rule, or to the same person or entity for a single purpose:
  - i. Although the DHS must provide a written accounting for disclosures made over a six year period, only the first disclosure made during the time period is necessary (the DHS need not list the same identical information for each subsequent disclosure to the same person or entity) if the DHS adds;
  - ii. The frequency or number of disclosures made to the same person or entity; and
  - iii. The last date of the disclosure made during the requested time period.
- i. **Provision of Accounting**: The DHS must act on the Client's request for an accounting no later than 60 days after receiving the request, subject to the following:
  - i. If unable to provide the accounting within 60 days after receiving the request, the DHS may extend this requirement by another 30 days. The DHS must provide the Client with a written statement of the reasons for the delay within the original 60-day limit, and inform the Client of the date by which the DHS may provide the accounting;
  - ii. The DHS may use only one such 30-day extension.
- j. **Fees**: The DHS must provide the first requested accounting in any 12-month period without charge. The DHS may charge the Client a reasonable cost-based fee for each additional accounting requested by the Client within the 12-month period following the first request, provided that the DHS:
  - i. Informs the Client of the fee before proceeding with any such additional request; and

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 13 of 14
		Issue/Revision Date April 14, 2003	

- ii. Allows the Client an opportunity to withdraw or modify the request in order to avoid or reduce the fee, multiple disclosures to the same person or entity for the same purpose, or as a result of a single written authorization by the Client.
- k. The DHS must document, and retain in the Client's DHS case record file, the information required to be included in an accounting of disclosures, the request for the accounting, and the titles of the persons who, or offices that, processed the accounting.
- l. **Suspension of Right to an Accounting:** The DHS may temporarily suspend a Client's right to receive an accounting of disclosures that the DHS has made to a health oversight agency or to a law enforcement official, for a length of time specified by such agency or official, if:
  - i. The agency or official provides a written statement to the DHS that such an accounting would be reasonably likely to impede their activities.
  - ii. However, if such agency or official makes an **oral** request, the DHS must:
    - A. Document the oral request, including the identity of the agency or official making the request;
    - B. Temporarily suspend the Client's right to an accounting of disclosures pursuant to the request; and
    - C. Limit the temporary suspension to no longer than 30 days from the date of the oral request, unless the agency or official submits a written request specifying a longer time period.

## 7. Rights of Clients to file complaints regarding disclosure of PHI

- a. Clients have a right to submit a complaint if they believe that the DHS has improperly used or disclosed their protected PHI, or if they have concerns about the privacy policies of the DHS or concerns about DHS compliance with such policies.
- b. Clients may file complaints with any of the following:
  - i. The DHS division that sent the Notice of Privacy Practices – the address is on the Notice.
  - ii. The State of Hawaii Department of Human Services  
DHS Privacy Officer  
P.O. Box 339  
Honolulu, HI 96809-0339  
Phone: 586-4954  
Email: dhs\_hipaa@dhs.state.hi.us

<b>DHS</b>  <b>P&amp;PM</b>	Subject Client Privacy Rights	Number 8.1.3	Page 14 of 14
		Issue/Revision Date April 14, 2003	

U. S. Department of Health and Human Services, Office for Civil Rights, Medical Privacy, Complaint Division

200 Independence Avenue, SW  
Washington, D.C. 20201  
Toll free Phone: 877-696-6775  
Phone: 866-627-7748  
TTY: 886-788-4989  
Email: [www.hhs.gov/ocr](http://www.hhs.gov/ocr)

- c. The DHS will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.
- d. The DHS will not require Clients to waive their rights to file a complaint as a condition of providing of treatment, payment, enrollment in a health plan, or eligibility for benefits.
- e. The DHS will designate staff to review and determine action on complaints filed with the DHS. These designated staff may also perform these functions when the DHS is contacted about complaints filed with the U.S. Department of Health and Human Services – the Office for Civil Rights.
- f. The DHS must document, in the Client's DHS case file or record, all complaints, the findings from reviewing each complaint, and the DHS actions resulting from the complaint. This documentation must include a description of corrective actions that the DHS has taken, if any are necessary, or of why corrective actions are not needed, for each specific complaint.

#### 4.0 SCOPE

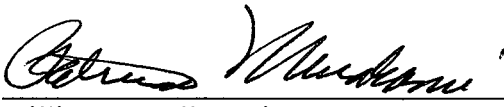
This policy applies to Covered Components of the DHS as listed in the Appendix B.

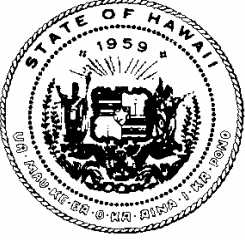
#### 5.0 RESPONSIBILITIES

Reserved for future use.

#### 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director

	Department of Human Services POLICIES AND PROCEDURES MANUAL		Number 8.1.4	Page 1 of 17
	Subject Uses and Disclosures of Client Information		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE:

The intent of this policy is to specify that Client Protected Health Information (PHI) cannot be used or disclosed by the Department of Human Services (DHS) without the Client's prior authorization, and to identify those exceptions that could be applicable.

## 2.0 REFERENCES AND DEFINITIONS:

### 2.1 REFERENCES

a.45 CFR 164.502(a), 508 –512

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A.

## 3.0 POLICY:

### 1. **General – Use and Disclosure**

The DHS may disclose PHI without Client authorization for purposes of DHS Treatment, Payment and Health Care Operations (TPO).

**Exception:** Release of PHI without authorization for TPO is limited by State and/or Federal law in cases of Clients with HIV/AIDS and those receiving mental health and substance abuse services, and such laws must be consulted and appropriate Client authorizations obtained, if necessary.

### 2. **General – Client Authorization**

- a. The DHS must not use or disclose any Client PHI without a signed authorization for release of that information from the Client, or the Client's legal representative, unless authorized by this policy, or as otherwise required by State or Federal law.
- b. The DHS must provide the Client with a copy of the signed authorization.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 2 of 17
		Issue/Revision Date April 14, 2003	

### 3. Valid Authorization

- a. The Client must agree to sign the authorization voluntarily.
- b. The DHS may not require the Client to sign an authorization as a condition of providing treatment services, payment for health care services, enrollment in a health plan, or eligibility for health plan benefits, except:

The DHS can require the Client to sign an authorization if the PHI needed will determine the applicant's eligibility for enrollment and the authorization is not for a use or disclosure of psychotherapy notes prior to enrolling the Client in a DHS health plan; or

The DHS and its contracted health care Providers can require the Client to sign an authorization before providing health care that is solely for the purpose of creating PHI for disclosure to a third party.

- c. An authorization that is required for enrollment in a health plan or to determine eligibility for benefits of the health plan cannot be combined with a voluntary authorization. A required authorization and a voluntary authorization must be separate documents, signed separately.
- d. DHS Staff must use the approved DHS, "Authorization to Disclose Confidential Information" forms.

The authorization must be written in plain language and must contain statements adequate to show that:

The Client's right to revoke the authorization in writing, and the exceptions to the right to revoke and a description of how the Client may revoke the authorization;

The DHS will not condition treatment, payment, enrollment or eligibility for benefits on whether or not the Client signs the authorization form, except as provided in subsection 3(b), above.

The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by this policy.

A valid authorization used or accepted by the DHS must contain the following core elements:

A description of the information to be used or disclosed, that identifies it in a specific and meaningful fashion;

The name or other specific information about the person(s), class of persons,



<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 3 of 17
		Issue/Revision Date April 14, 2003	

or entity (i.e., the DHS or specified DHS Covered Component) authorized to make the specific use or disclosure;

The name or other specific identification of the person(s), classification of persons, or entity to whom the DHS may make the requested use or disclosure;

A description of each purpose of the requested use or disclosure;

An expiration date, or an expiration event that relates to the Client or to the purpose of the use or disclosure;

Signature of the Client, or of the Client's legal representative, and the date of signature;

If the Client's legal representative signs the authorization form instead of the Client, a description or explanation of the representative's authority to act for the Client, including a copy of the legal court document (if any) appointing the legal representative, must also be provided.

If the DHS authorization forms allow for multiple releases on one form, the Client has the right to request that only one release be requested per form. The DHS will always honor the request;

The DHS must document and retain each signed Authorization Form for a minimum of six years.

e. An authorization is considered invalid if:

The expiration date is not present, has expired or the expiration event is known by the DHS to have occurred;

The authorization has not been filled out completely;

The authorization is known by the DHS to have been revoked;

An authorization conditions treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, other than as provided in subsection 3(a), above;

Any material information in the authorization is known by the DHS to be false.

#### 4. **When an Authorization is required**

a. Except as otherwise permitted or required by law and consistent with these policies, the DHS must obtain a completed and signed authorization for release of PHI from

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 4 of 17
		Issue/Revision Date April 14, 2003	

the Client, or the Client's legal representative, before obtaining or using PHI about a Client from a third party or disclosing any information about the Client to a third party.

A signed authorization is required in the following situations:

Prior to a Client's enrollment in a DHS administered health plan, if necessary for determining eligibility or enrollment;

For the use and disclosure of psychotherapy notes (for exception see subsection 8 of this policy);

For disclosures to an employer for use in employment-related determinations; and

For research purposes unrelated to the Client's treatment (see DHS Privacy Policy No. 8.1.5, "Uses and Disclosures for Research Purposes").

For any purpose in which State or Federal law requires a signed authorization.

- b. Uses and disclosures must be consistent with what the Client has authorized on a signed authorization form.

#### 5. **Limited uses or disclosures that are allowed without authorization that require tracking**

The DHS must track certain disclosures of PHI that are permitted without Client authorization in order to provide the Client with an accounting of disclosures in accordance with DHS Privacy Policy No. 8.1.3, "Client Privacy Rights" section 3.6.

- a. **Required by Law:** The DHS may use or disclose PHI without a Client's authorization to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
- b. **Public Health:** The DHS may disclose PHI for the public health activities and purposes described in this paragraph to:

A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 5 of 17
		Issue/Revision Date April 14, 2003	

- c. **Abuse and Neglect:** The DHS may disclose PHI to a public health authority or other appropriate government authority authorized by law to receive reports of child or elder abuse or neglect as follows:

If DHS Staff has reasonable cause to believe that a child is a victim of abuse or neglect, the DHS may disclose PHI to appropriate governmental authorities authorized by law to receive reports of child abuse or neglect (including reporting to DHS protective services staff, if appropriate). If the DHS receives information as the child protective services agency, the DHS is authorized to use and disclose the information consistent with its legal authority.

If the DHS has reasonable cause to believe that an adult is a victim of abuse, neglect, or domestic violence (elder abuse, nursing home abuse, or abuse of the mentally ill or developmentally disabled), the DHS may disclose PHI to a government authority, including a social service or protective services agency (which may include the DHS), authorized by law to receive reports of such abuse or neglect:

If the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or

If the Client authorizes the disclosure, either orally or in writing; or

To the extent authorized by law, when DHS Staff, in the exercise of professional judgment and in consultation with appropriate DHS supervisor, believes the disclosure is necessary to prevent serious harm to the Client or other persons; or

To the extent authorized by law, when the Client is unable to agree because of incapacity, a law enforcement agency or other public official authorized to receive the report represents that:

The PHI being sought is not intended to be used against the Client, and

An immediate law enforcement activity would be materially and adversely affected by waiting until the Client is able to agree to the disclosure.

When DHS Staff disclose PHI as permitted in subsection 5(c) above, the DHS must promptly inform the Client that such a report has been or will be made, except if:

DHS Staff, in the exercise of professional judgment and in consultation with the appropriate DHS supervisor, believes informing the Client would place the Client or another Client at risk of serious harm; or

DHS Staff would be informing a legal representative and DHS Staff

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 6 of 17
		Issue/Revision Date April 14, 2003	

reasonably believes the legal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the Client, as determined by DHS Staff, in the exercise of professional judgment and in consultation with the appropriate DHS supervisor.

- d. **Health Oversight:** The DHS may disclose PHI without authorization for Health Oversight activities authorized by law, including audits; inspections; civil, criminal, or administrative investigations, prosecutions, or actions; licensing or disciplinary actions; Medicaid fraud; or other activities.

The DHS may disclose PHI to a Health Oversight agency to the extent the disclosure is not prohibited by State or Federal law.

**Exception:** a Health Oversight activity for which information may be disclosed does *not* include an investigation or other activity of which the Client is the subject *unless* the investigation or other activity is directly related to:

The receipt of health care;

A claim to recover public benefits related to health; or

Qualifying for or receiving public benefits or services based on the health of the Client.

If a Health Oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity is considered a Health Oversight activity for purposes of this section.

When the DHS or one of its organizational units is acting as a Health Oversight agency, the DHS may use PHI for Health Oversight activities as permitted under this section.

- e. **Judicial and Administrative Proceedings:** Unless prohibited, or otherwise limited, by State or Federal law applicable to the program or activity requirements, the DHS may disclose Client PHI without authorization for judicial or administrative proceedings, in response to an order of a court or administrative tribunal, a subpoena, a discovery request or other lawful process.

The DHS may disclose PHI in the course of any judicial or administrative proceeding as follows:

In response to an order of a court or administrative tribunal, provided that the DHS discloses only the PHI expressly authorized by such order; or

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 7 of 17
		Issue/Revision Date April 14, 2003	

In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

**Notice to the Client:** The DHS receives satisfactory assurance from the requestor that reasonable efforts have been made to ensure that the Client who is the subject of the PHI has been given notice of the request; or

**Qualified Protective Order:** The DHS receives satisfactory assurance from the requestor that reasonable efforts have been made to secure a qualified protective order.

The DHS receives satisfactory assurance from the requestor that reasonable efforts have been made to ensure that the Client who is the subject of the PHI has been given notice of the request by submitting to the DHS a written statement and accompanying documentation demonstrating that:

- (a) The requestor has made a good faith attempt to provide written notice to the Client (or, if the Client's location is unknown, to mail a notice to the Client's last known address);
- (b) The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the Client to raise an objection to the court or administrative tribunal; and
- (c) The time for the Client to raise objections to the court or administrative tribunal has elapsed, and no objections were filed, or all objections filed by the Client have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

If the DHS receives satisfactory assurances from a requestor in the form of a written statement and accompanying documentation demonstrating that:

The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

The requestor has requested a qualified protective order from such court or administrative tribunal.

**Qualified Protective Order Requirements:** A qualified protective order means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 8 of 17
		Issue/Revision Date April 14, 2003	

Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and

Requires the return to the DHS or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

The DHS may disclose PHI in response to the lawful processes described above without receiving the satisfactory assurances described above, if the DHS makes reasonable efforts to provide notice to the Client or to seek a qualified protective order.

The DHS must verify the identity of all requestors who request PHI in judicial and administrative proceedings (see section 12 of this policy).

The provisions of this part do not supersede other provisions of this policy section that otherwise permit or restrict uses or disclosures of PHI.

- f. **Law Enforcement:** For limited law enforcement purposes, to the extent authorized by applicable State or Federal law, the DHS may: 1) report certain injuries or wounds; 2) provide PHI to identify or locate a suspect, fugitive, victim, witness, or missing person; 3) alert law enforcement of a death as a result of criminal conduct; and 4) provide information which constitutes evidence of criminal conduct on the DHS premises.
  - i. The DHS may disclose PHI for a law enforcement purpose to a law enforcement official as follows:
    - A. **Required by Law:** In compliance with and as limited by the relevant requirements of:
 

A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

A grand jury subpoena; or

An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

      - (a) The information sought is relevant and material to a legitimate law enforcement inquiry;
      - (b) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 9 of 17
		Issue/Revision Date April 14, 2003	

(c) De-identified information could not reasonably be used.

**B. Identification and Location Purposes:** Except for disclosures required by law as permitted in part A above, the DHS may disclose PHI in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

I. The DHS may disclose only the following information:

- (a) Name and address;
- (b) Date and place of birth;
- (c) Social security number;
- (d) ABO blood type and Rh factor;
- (e) Type of injury;
- (f) Date and time of treatment;
- (g) Date and time of death, if applicable; and
- (h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

II. Except as permitted above, the DHS may **not** disclose for the purposes of identification or location any PHI related to the Client's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

g. **Victims of Crime:** DHS may disclose protected information upon request to a law enforcement official about an individual who is or is suspected to be the victim of a crime, if:

- i. DHS is otherwise authorized by law to disclose that information for purposes of an abuse reporting law or for public health or health oversight purposes; or
- ii. The individual agrees to the disclosure, either orally or in writing; or
- iii. DHS is unable to obtain the individual's agreement due to incapacity or emergency circumstance, if:

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 10 of 17
		Issue/Revision Date April 14, 2003	

- A. The law enforcement official represents that such information is needed to determine whether a violation of law by someone other than the victim has occurred and such information is not intended for use against the victim;
  - B. The law enforcement official represents that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
  - C. DHS determines that the disclosure is in the best interests of the individual.
- h. **Client who has Died:** The DHS may disclose PHI about a Client who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the Client if the DHS has a suspicion that such death may have resulted from criminal conduct.
  - i. **Crime on DHS Premises:** Use and disclosure of Client PHI to a law enforcement official is permitted in the event that a DHS Staff member who is the victim of a criminal act believes in good faith that the PHI constitutes evidence of criminal conduct that occurred on the premises of the DHS provided that:
    - i. The PHI disclosed is about the suspected perpetrator of the criminal act; and
    - ii. The PHI disclosed is limited to the information listed in subsection f (i)(B), above.
  - j. **Coroner or Medical Examiner:** The DHS may disclose to a coroner or medical examiner, for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law.
  - k. **Funeral Directors:** The DHS may disclose Client PHI without authorization to funeral directors, consistent with applicable law, as needed to carry out their duties regarding the decedent. The DHS may also disclose such information prior to, and in reasonable anticipation of, the death, if necessary for funeral directors to carry out their duties.
  - l. **Organ Procurement:** The DHS may disclose Client PHI without authorization to organ procurement organizations or other entities engaged in procuring, banking, or transplantation of cadaver organs, eyes, or tissue, for the purpose of facilitating transplantation.
  - m. **Research:** The DHS may disclose Client PHI without authorization for research purposes, only as specified in DHS Privacy Policy No. 8.1.5, "Uses and Disclosures for Research Purposes."
  - n. **Threat to Health or Safety:** To avert a serious threat to health or safety, the DHS may disclose Client PHI without authorization if:



<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 11 of 17
		Issue/Revision Date April 14, 2003	

- i. The DHS believes in good faith that the information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the report is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
    - ii. The PHI is necessary for law enforcement to authorities to apprehend or identify a Client.
  - o. **Specialized Government Functions:** The DHS may disclose a Client's PHI without Client authorization for Clients who are Armed Forces personnel, as deemed necessary by appropriate military command authorities to ensure the proper execution of the military mission, unless such disclosure is prohibited by State or Federal law.
6. **Disclosures that are not required to be tracked and accounted for are those that are:**
- a. For purposes of TPO as specified in Section 1 of this policy.
- Exception:** Release of PHI without authorization for TPO is limited by state and/or federal law in cases of Clients with HIV/AIDS and those receiving mental health and substance abuse services, and such laws must be consulted and appropriate Client authorizations obtained, if necessary.
- b. Authorized by the Client;
  - c. Made prior to the original effective date of this policy, which is April 14, 2003;
  - d. Made to persons identified by the Client as permitted to receive PHI relevant to such person's involvement with the Client's health care or payment;
  - e. Made as part of a limited data set in accordance with DHS Privacy Policy No. 8.1.7, "De-identification of Client Information and Use of Limited Data Sets".
7. **Limited uses or disclosures that are allowed without authorization that are not required to be tracked**
- a. The DHS may disclose PHI without authorization to another Covered Entity for the health care activities of that entity, if:
    - i. Both that entity and the DHS has or has had a relationship with the Client who is the subject of the PHI;
    - ii. The information pertains to such relationship; and
    - iii. The disclosure is for the purpose of:

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 12 of 17
		Issue/Revision Date April 14, 2003	

- A. Conducting quality assessment and improvement activities, including: outcome evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting Health Care Providers and patients with information about treatment alternatives; and related functions that do not include treatment; or
  - B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improvement their skills as Health Care Providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities;
- b. The DHS may disclose PHI relating to eligibility for or enrollment in a health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.
  - c. Internal communication within the DHS is permitted without Client authorization, in compliance with DHS Privacy Policy No. 8.1.6, "Minimum Necessary Information."
  - d. DHS Clients may access their own PHI, with certain limitations (see DHS Privacy Policy No. 8.1.3, "Client Privacy Rights").
  - e. The DHS may disclose Client PHI without authorization for the conduct of lawful intelligence, counterintelligence, and other national security activities that federal law authorizes.
  - f. The DHS may disclose limited PHI without authorization to correctional institutions or law enforcement officials having lawful custody of a Client who is an inmate if the correctional institution or such law enforcement official represents that such PHI is necessary for:
    - i. The provision of health care to such Client;
    - ii. The health and safety of such Client or other inmates;
    - iii. The health and safety of the officers or employees of or others at the

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 13 of 17
		Issue/Revision Date April 14, 2003	

correctional institution;

- iv. The health and safety of such Client and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
- v. Law enforcement on the premises of the correctional institution; and
- vi. The administration and maintenance of the safety, security, and good order of the correctional institution.

**Note:** A Client is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

## 8. Psychotherapy notes

- a. The DHS may use or disclose a Client's psychotherapy notes without Client authorization as follows:
  - i. To the extent that the use or disclosure is required by State or Federal Law and the use or disclosure complies with and is limited to the relevant requirements of that law.
  - ii. When the DHS uses or discloses in connection with oversight of the originator of the psychotherapy notes; or
  - iii. To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
  - iv. Consistent with applicable law and standards of ethical conduct, use or disclosure of PHI, if the DHS, in good faith, believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.
  - v. To the extent authorized under state law to defend the DHS in a legal action or other proceeding brought by the Client;
  - vi. Only for use by the originator of the psychotherapy notes, for treatment purposes.

## 9. Use or Disclosure of PHI that does not require an authorization if the client is informed in advance and given a chance to object

- a. In limited circumstances, the DHS may use or disclose a Client's PHI without authorization if:


<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 14 of 17
		Issue/Revision Date April 14, 2003	

- i. The DHS informs the Client in advance and the Client has been given an opportunity to object;
  - ii. Unless otherwise protected by law, the DHS may orally inform the Client and obtain and document the Client's oral agreement.
- b. These Disclosures are limited to disclosure of PHI to a family member, other relative, or close personal friend of the Client, or any other person named by the Client. Disclosures may be made in this circumstance subject to the following limitations:
  - i. The DHS may reveal only the PHI that directly relates to such person's involvement with the Client's care or payment for such care;
  - ii. The DHS may use or disclose PHI for notifying (including identifying or locating) a family member, legal representative, or other person responsible for care of the Client, about the Client's location, general condition, or death.
  - iii. If the Client is present for or available prior to, such a use or disclosure, the DHS may disclose the PHI if it:
    - A. Obtains the Client's agreement;
    - B. Provides the Client an opportunity to object to the disclosure, and the Client does not express an objection; or
    - C. Reasonably infers from the circumstances that the Client does not object to the disclosure.
  - iv. If the Client is not present, or the opportunity to object to the use or disclosure cannot practicably be provided due to the Client's incapacity or an emergency situation, the DHS may determine, using professional judgment, that the use or disclosure is in the Client's best interests.
    - A. Any agreement, objection, refusal, or restriction by the Client, may be oral or in writing. The DHS will document any such oral communication in the Client's case file.
    - B. The DHS will also document in the case file the outcome of any opportunity provided to object; the Client's decision not to object; or the inability of the Client to object.
- c. Oral permission to use or disclose PHI for the purposes described in subsections (a) of this section is not sufficient when the Client is referred to or receiving substance abuse treatment services or mental health treatment services, where written authorization for the treatment program to make such disclosures is required.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 15 of 17
		Issue/Revision Date April 14, 2003	

- d. The DHS can disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The DHS may exercise professional judgment to determine that this requirement does not interfere with the ability to respond to the emergency circumstances.

#### 10. Re-disclosure of a Client's Information:

- a. Unless prohibited by State or Federal law, PHI held by the DHS and authorized by the Client for disclosure may be subject to re-disclosure and no longer protected by the DHS Privacy Policies. Whether or not the PHI remains protected depends on whether the recipient is subject to State or Federal privacy laws, court protective orders or other lawful process.
- b. Alcohol and Drug Rehabilitation information: Federal regulations (42 CFR part 2) prohibit the DHS from making further disclosure of certain alcohol and drug rehabilitation information without the specific written authorization of the Client to whom it pertains.
- c. State laws hibit the further disclosure of HIV information.
- d. State law limits further disclosure of genetic information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. A general authorization for the release of medical information is not sufficient for this purpose.
- e. State law places restrictions on re-disclosure of information regarding Clients of publicly funded mental health or developmental disability providers.

#### 11. Revocation of Authorization

- a. A Client can revoke an authorization at any time.
- b. Any revocation must be in writing and signed by the Client.
- c. A revocation will not apply to PHI released while the authorization was valid and in effect.
- d. Documentation of authorizations and revocations must be retained by the DHS for a minimum of six years.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures of Client Information	Number 8.1.4	Page 16 of 17
		Issue/Revision Date April 14, 2003	

## 12. Verifying Identity of Requestors of PHI

- a. All requests for PHI about a Client, including information contained in limited data sets and information requested by Clients, will require verification of the identity of the person requesting the PHI prior to disclosure.
- b. Acceptable assumptions of the identification and authorization of requests for PHI by DHS Staff include the provisions listed below:
  - i. If a disclosure is conditioned on particular documentation, statements, or representations from the person requesting the PHI, the DHS may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements;
  - ii. The administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met;
  - iii. The documentation may be satisfied by one or more written statements, provided that each is appropriately dated and signed.
- c. If disclosing PHI to a Public Official or a person acting on behalf of a Public Official, DHS staff will need to verify their identity.
  - i. If the request is in person, presentation of an agency identification badge or other official credentials of governmental status is required.
  - ii. If the request is in writing, the request must be on appropriate government letterhead.
  - iii. If the disclosure is to a person acting on behalf of the Public Official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, Memorandum of Understanding (MOU), or purchase order, that establishes that the person is acting on behalf of the Public Official.
    - A. Public Officials have authority to receive PHI when a written statement of the legal authority is provided or if the written statement is impracticable, an oral statement of legal authority; or
    - B. The request from the Public Official is pursuant to a legal process, warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal is presumed to constitute legal authority.

<b>DHS</b>  <b>P&amp;PM</b>	<b>Subject</b> <b>Uses and Disclosures of Client</b> <b>Information</b>	<b>Number</b> 8.1.4	<b>Page</b> 17 of 17
		<b>Issue/Revision Date</b> April 14, 2003	

### 13. Denial of Requests for PHI

Unless a Client has signed an authorization, or the information about the Client can be disclosed without an authorization pursuant to this policy, the DHS must deny any request for PHI.

#### 4.0 SCOPE


This policy applies to Covered Components of the DHS as listed in the Appendix B.

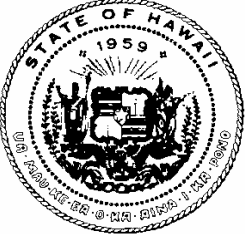
#### 5.0 RESPONSIBILITIES

Reserved for future use.

#### 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director

	<b>Department of Human Services</b> <b>POLICIES AND PROCEDURES</b> <b>MANUAL</b>		Number 8.1.5	Page 1 of 3
	Subject Uses and Disclosures for Research Purposes		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE:

The intent of this policy is to specify when the Department of Human Services (DHS) may use or disclose Protected Health Information (PHI) about Clients for Research purposes.

## 2.0 REFERENCES AND DEFINITIONS:

### 2.1 REFERENCES

- a. 45 CFR Part 46
- b. 45 CFR 164.501, 508, 512 and 528

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A

## 3.0 POLICY:

### 1. General

When the DHS uses or discloses a Client's PHI for Research purposes, it must consider the following:

- a. The DHS will use or disclose a Client's PHI for Research purposes only as specified in this policy.
- b. All such Research disclosures are subject to applicable requirements of State and Federal laws and to the specific requirements of this policy.

**Note:** This policy is intended to supplement existing Research requirements of the Common Rule, 45 CFR Part 46. The Common Rule is the rule for the protection of human subjects in Research promulgated by the U.S. Department of Health and Human Services, and adopted by other federal governmental agencies, including the National Institutes for Health, for Research funded by those agencies. In addition, some agencies have requirements that supplement the Common Rule that are applicable to a particular Research contract or grant.

- c. De-identified information will be used or disclosed for purposes of Research, consistent with Section 8.1.7 of the DHS Privacy Policies, "De-identification of



<b>DHS</b>  <b>P&amp;PM</b>	Subject Uses and Disclosures for Research Purposes	Number 8.1.5	Page 2 of 3
		Issue/Revision Date April 14, 2003	

Client Information and Use of Limited Data Sets.”


- d. A Limited Data Set may be used or disclosed for purposes of Research, consistent with the DHS Privacy Policies related to Limited Data Sets in DHS Privacy Policy No. 8.1.7, “De-identification of Client Information and Use of Limited Data Sets.”
- e. The DHS may also conduct program evaluation studies, studies that are required by law, and studies or analysis related to its Health Care Operations or Health Care Oversight. Such studies will be discussed in Sections (3.) and (4.) of this policy.

## **2. Uses and disclosures for Research purposes – specific requirements**

- a. The DHS may use or disclose Client PHI for Research purposes with the Client’s specific written authorization.
  - i. Such authorization must meet all the requirements described in Section 8.1.4 of the DHS Privacy Policies, “Uses and Disclosures of Client Information,” and will indicate as an expiration date such terms as “end of Research study,” or similar language.
  - ii. An authorization for use and disclosure for a Research study may be combined with any other type of written permission for the same Research study.
  - iii. If Research includes treatment, the researcher may condition the provision of Research related treatment on the provision of an authorization for use and disclosure for such Research.

## **3. DHS Studies Related to Health Care Operations or Health Oversight**

- a. Client authorization is not required for studies or data analyses conducted by or on behalf of the DHS for purposes of Health Care Operations or Health Oversight, including any studies or analyses conducted to comply with reporting requirements applicable to state or federal funding requirements.

 **Exception:** HIV-AIDS information will not be disclosed to anyone without the specific written authorization of the Client. Re-disclosure of HIV test information is prohibited, except in compliance with State or Federal Law or with written permission from the Client.

<b>DHS</b>  <b>P&amp;PM</b>	<b>Subject</b> <b>Uses and Disclosures for Research Purposes</b>	<b>Number</b> 8.1.5	<b>Page</b> 3 of 3
		<b>Issue/Revision Date</b> April 14, 2003	

#### 4. Accounting for Disclosures for Research purposes

- a. Uses and Disclosures of PHI for Research purposes do not need to be tracked in an accounting if conducted pursuant to a valid Client Authorization (See DHS Privacy Policy No. 8.1.3, "Client Privacy Rights" section 3.6.f.i).
- b. Uses and Disclosures of PHI for DHS Health Care Operations do not need to be tracked in an accounting (see DHS Privacy Policy No. 8.1.3, "Client Privacy Rights" section 3.6.f.iii, and DHS Privacy Policy No.8.1.4, "Uses and Disclosures of Client Information" section 3.6.a).
- c. Uses and Disclosures of PHI for Health Oversight must be tracked in an accounting (see DHS Privacy Policy No. 8.1.3, "Client Privacy Rights" section 3.6.g.iv).

#### 4.0 SCOPE


This policy applies to Covered Components of the DHS as listed in the Appendix B.

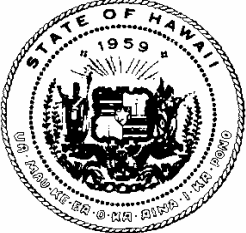
#### 5.0 RESPONSIBILITIES

Reserved for future use.

#### 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director

	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.1.6	Page 1 of 3
	Subject Minimum Necessary Information		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE

The intention of the Department of Human Services (DHS) Minimum Necessary Information Policy is to:

- Improve the privacy of Protected Health Information (PHI) that is used or disclosed by DHS Staff in the course of their work; and
- Ensure that DHS Staff have access to the PHI they require to accomplish the mission, goals and objectives of the DHS.

## 2.0 REFERENCES AND DEFINITIONS

### 2.1 REFERENCES

- (a) 45 CFR Parts 164.502 and 164.514

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A.

## 3.0 POLICY

### 1. General

- a. The DHS must use or disclose only the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure or request to the extent provided in DHS policies and procedures.
- b. This policy does not apply to:
  - i. Disclosures to or requests by a health care provider for treatment;
  - ii. Disclosures made to a Client about his or her own PHI;
  - iii. Uses or disclosures authorized by a Client or Client's legal representative;
  - iv. Disclosures made to the United States Department of Health and Human Services (DHHS), Office of Civil Rights (OCR), for compliance with and enforcement of the HIPAA Privacy Rule;
  - v. Uses or disclosures that are required by law;
  - vi. The required or situational data elements specified in the implementation guides under the HIPAA Transaction and Code Sets Rule, Part 162 (as specified in the HIPAA Privacy Rule Vol. 65 Preamble, p. 82545).

<b>DHS</b>  <b>P&amp;PM</b>	Subject Minimum Necessary Information	Number 8.1.6	Page 2 of 3
		Issue/Revision Date April 14, 2003	

## **2. DHS Staff to access PHI**

- a. The DHS must establish Role-Based Access categories that:
  - i. Identify DHS Staff by role categories that need access to PHI;
  - ii. Identify categories of PHI that Staff must access, and conditions on such access;
  - iii. Establish procedures to limit access of such DHS Staff to the minimum necessary.
- b. The access categories include DHS Staff access to all information, including PHI accessible by computer, kept in files, or other forms of PHI consistent with DHS Privacy Policy No. 8.1.8, "Administrative, Technical and Physical Safeguards."

## **3. Minimum Necessary Requirements: Disclosures by the DHS**

- a. When DHS Policy permits use or disclosure of a Client's PHI to another entity, or when DHS requests a Client's PHI from another entity, DHS Staff must make reasonable efforts to limit the amount of PHI to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.
- b. If DHS Policy permits making a particular disclosure to another entity, DHS Staff must rely on a requested disclosure as being the minimum necessary for the stated purpose when:
  - i. Making disclosures to Public Officials that are permitted, and as listed in DHS Privacy Policy No. 8.1.4, "Uses and Disclosures of Client Information," if the Public Official represents the PHI requested is the minimum necessary for the stated purpose(s).
  - ii. The PHI is requested by another entity that is a "Covered Entity" under the HIPAA Privacy Rule.
  - iii. The PHI is requested by a professional who is a member of DHS Staff or is a business associate of the DHS for the purpose of providing professional services to the DHS, if the professional represents that the PHI requested is the minimum necessary for the stated purpose(s); or
  - iv. The requestor provides documentation or representations that the disclosure is for research purposes, in accordance with DHS Privacy Policy No. 8.1.5, "Uses and Disclosures for Research Purposes".
- c. The DHS must not disclose a Client's entire medical record unless the request specifically justifies why the entire medical record is needed, and applicable laws and policies permit the disclosure of all of the information contained in the medical record to the requestor.

## **4. Routine and Recurring Disclosure of PHI**

- a. The DHS must implement policies and procedures that limit the disclosure of PHI to the amount reasonably necessary to achieve the purpose of any Routine and Recurring disclosure.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Minimum Necessary Information	Number 8.1.6	Page 3 of 3
		Issue/Revision Date April 14, 2003	

**5. Non-Routine Disclosure of a Client's PHI:**

- a. For non-routine disclosures, the DHS must:
  - i. Develop criteria designed to limit the PHI disclosed to only the amount of information reasonably necessary to accomplish the purpose for which the disclosure is sought; and
  - ii. Review requests for non-routine disclosures on an individual basis in accordance with such criteria.

**6. Minimum Necessary Requirements: DHS Requests for Client PHI from another Covered Entity**

- a. When requesting information about a Client from another Covered Entity, DHS Staff must limit requests to those that are reasonably necessary to accomplish the purpose for which the request is made.
- b. For Routine and Recurring requests, the DHS must implement policies and procedures to limit the information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.
- c. For all other requests, the DHS must:
  - i. Develop criteria to limit the information requested to the amount of information reasonably necessary to accomplish the purpose for which the request is made; and
  - ii. Review requests for disclosure on an individual basis in accordance with such criteria.
- d. The DHS must not request a Client's entire medical record unless the DHS can specifically justify why the entire medical record is needed.

**4.0 SCOPE**



This policy applies to Covered Components of the DHS as listed in the Appendix B.

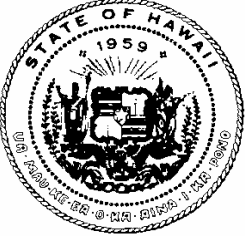
**5.0 RESPONSIBILITIES**

Reserved for future use.

**6.0 DESCRIPTIVE PARAGRAPHS**

Reserved for future use.

APPROVED:   
 Lillian B. Koller, Director

	<b>Department of Human Services</b> <b>POLICIES AND PROCEDURES</b> <b>MANUAL</b>		Number 8.1.7	Page 1 of 6
	Subject De-identification of Client Information and Use of Limited Data Sets		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE:

The intent of this policy is to prescribe standards under which Client information can be used and disclosed if information that can identify a person has been removed or restricted to a Limited Data Set.

## 2.0 REFERENCES AND DEFINITIONS:

### 2.1 REFERENCES

- a. 45 CFR 164.502 and 514

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A

## 3.0 POLICY

### 1. General

- a. De-identified Information is Client Protected Health Information (PHI) from which the Department of Human Services (DHS) or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify the Client.
- b. Unless otherwise restricted or prohibited by other State or Federal law, the DHS can use and share information as appropriate for the work of the DHS, without further restriction, if the DHS or another entity has taken steps to de-identify the information consistent with the requirements and restrictions of Section (2.) of this policy
- c. The DHS may use or disclose a Limited Data Set that meets the requirements of Section (4.) of this policy, if the DHS enters into a Data Use Agreement with the Limited Data Set recipient (or with the data source, if the DHS may be the recipient of the Limited Data Set) in accordance with the requirements of Section (5.) of this policy.

<b>DHS</b>  <b>P&amp;PM</b>	Subject De-identification of Client Information and Use of Limited Data Sets	Number 8.1.7	Page 2 of 6
		Issue/Revision Date April 14, 2003	

- d. The DHS will disclose a Limited Data Set only for the purposes of research, or non-governmental public health purposes. However, unless the DHS has obtained a Limited Data Set that is subject to a Data Use Agreement, the DHS is not restricted to using a Limited Data Set for its own activities or operations.
- e. If the DHS knows of a pattern or activity or practice of the Limited Data Set recipient that constitutes a material breach or violation of a data set agreement, the DHS will take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, the DHS will discontinue disclosure of information to the recipient and report the problem to the United States Department of Health and Human Services (DHHS), Office of Civil Rights.

## 2. Requirements for de-identification of Client information

- a. The DHS may determine that Client information is sufficiently de-identified, and cannot be used to identify a Client, only if **either** (i.) or (ii.) below have occurred:
  - i. The DHS has ensured that:
    - A. The following identifiers of the Client or of relatives, employers, and household members of the Client are removed:
      - I. Names;
      - II. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code will remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;
      - III. All elements of dates (except year) for dates directly relating to a Client, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 89 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements will be aggregated into a single category of "age 89 or older;"
      - IV. Telephone numbers;
      - V. Fax numbers;
      - VI. Electronic mail addresses;

<b>DHS</b>  <b>P&amp;PM</b>	Subject De-identification of Client Information and Use of Limited Data Sets	Number 8.1.7	Page 3 of 6
		Issue/Revision Date April 14, 2003	

- VII. Social security numbers;
  - VIII. Medical record numbers;
  - IX. Health plan beneficiary numbers;
  - X. Account numbers;
  - XI. Certificate or license numbers;
  - XII. Vehicle identifiers and serial numbers, including license plate numbers;
  - XIII. Device identifiers and serial numbers;
  - XIV. Web Universal Resource Locators (URLs);
  - XV. Internet Protocol (IP) address numbers;
  - XVI. Biometric identifiers, including fingerprints and voiceprints;
  - XVII. Full face photographic images and any comparable images; and
  - XVIII. Any other unique identifying number, characteristic, or codes, except as permitted under Section (3.), below, of this policy; **and**
- B. The DHS has no actual knowledge that the information could be used alone or in combination with other information to identify a Client who is the subject of the information.
- ii. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
    - A. Has applied such principles and methods, and determined that the risk is minimal that the information could be used, alone or in combination with other reasonably available information, by a recipient of the information to identify the person whose information is being used; and
    - B. Has documented the methods and results of the analysis that justify such a determination; or
  - b. The DHS will designate the statistician or other person referred to in (2.)(a.)(i.), above, who will be either:
    - i. DHS Staff;



<b>DHS</b>  <b>P&amp;PM</b>	Subject De-identification of Client Information and Use of Limited Data Sets	Number 8.1.7	Page 4 of 6
		Issue/Revision Date April 14, 2003	

- ii. An employee of another governmental agency; or
- iii. An outside contractor or consultant, subject to DHS contracting and personnel policy, including in conformance with Business Associate provisions, as set forth in DHS Privacy Policy No. 8.1.2, "Business Associate Relationships".

### **3. Re-identification of De-identified Information**

- a. The DHS may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by the DHS, except that:
  - i. The code or other means of record identification is not derived from or related to information about the Client and cannot otherwise be translated to identify the Client; and
  - ii. The DHS does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

### **4. Requirements for a Limited Data Set**

- a. A Limited Data Set is information that excludes the following direct identifiers of the Client, or of relatives, employers or household members of the Client:
  - i. Names;
  - ii. Postal address information, other than town or city, State and zip code;
  - iii. Telephone numbers;
  - iv. Fax numbers;
  - v. Electronic mail addresses;
  - vi. Social Security numbers;
  - vii. Medical record numbers;
  - viii. Health plan beneficiary numbers (such as Medicaid Prime Numbers);
  - ix. Account numbers;
  - x. Certificate/license numbers;
  - xi. Vehicle identifiers and serial numbers, including license plate numbers;

<b>DHS</b>  <b>P&amp;PM</b>	Subject De-identification of Client Information and Use of Limited Data Sets	Number 8.1.7	Page 5 of 6
		Issue/Revision Date April 14, 2003	

- xii. Web Universal Resource Locators (URLs);
- xiii. Internet Protocol (IP) address numbers;
- xiv. Biometric identifiers, including finger and voice prints; and
- xv. Full face photographic images and any comparable images.

## 5. Contents of a Data Use Agreement

- a. The DHS will disclose a Limited Data Set only if the entity receiving the Limited Data Set enters into a written agreement with the DHS, in accordance with subsection (5.)(b.) immediately below, that such entity will use or disclose the PHI only as specified in the written agreement.
- b. A Data Use Agreement between the DHS and the recipient of the Limited Data Set must:
  - i. Specify the permitted uses and disclosures of such information by the Limited Data Set recipient. The DHS will not use the agreement to authorize the Limited Data Set recipient to use or further disclose the information in a manner that would violate the requirements of this policy if done by the DHS.
  - ii. Specify who is permitted to use or receive the Limited Data Set; and
  - iii. Specify that the Limited Data Set recipient will:
    - A. Not use or further disclose the information other than as specified in the Data Use Agreement or as otherwise required by law;
    - B. Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the Data Use Agreement;
    - C. Report to the DHS, if the DHS is the source of the Limited Data Set, if the recipient becomes aware of any use or disclosure of the information not specified in its Data Use Agreement with the DHS;
    - D. Ensure that any agents, including a subcontractor, to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information; and
    - E. Not identify the information or contact the Clients whose data is being disclosed.

<b>DHS</b>  <b>P&amp;PM</b>	<b>Subject</b> <b>De-identification of Client Information</b> <b>and Use of Limited Data Sets</b>	<b>Number</b> 8.1.7	<b>Page</b> 6 of 6
		<b>Issue/Revision Date</b> April 14, 2003	

#### 4.0 SCOPE

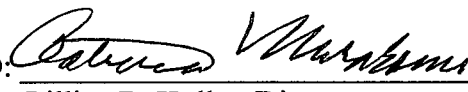
This policy applies to Covered Components of the DHS as listed in the Appendix B.

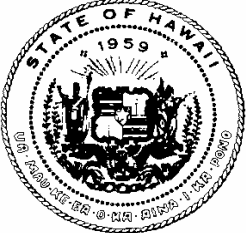
#### 5.0 RESPONSIBILITIES

Reserved for future use.

#### 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director

	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.1.8	Page 1 of 3
	Subject Administrative, Technical and Physical Safeguards		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE

The intent of this policy is to establish criteria for safeguarding Protected Health Information (PHI) and to minimize the risk of unauthorized access, use or disclosure.

## 2.0 REFERENCES AND DEFINITIONS

### 2.1 REFERENCES

- a. 45 CFR 164.530(c)(1)

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A

## 3.0 POLICY

### 1. General

- a. The Department of Human Services (DHS) must take reasonable steps to safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the DHS Privacy Policies.
- b. Information to be safeguarded may be in any medium, including paper.

### 2. DHS workplace practices

- a. Paper:
  - i. Each DHS workplace must store files and documents in locked rooms or storage systems.
  - ii. In workplaces where lockable storage is not available, DHS Staff must take reasonable efforts to ensure the safeguarding of PHI.
  - iii. Each DHS workplace must ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
  - iv. Each DHS workplace must ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Administrative, Technical and Physical Safeguards	Number 8.1.8	Page 2 of 3
		OPR Director's Office	
		Issue/Revision Date April 14, 2003	

b. Oral:

- i. DHS Staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of PHI, regardless of where the discussion occurs.
- ii. Each DHS workplace must foster employee awareness of the potential for inadvertent verbal disclosure of PHI and make available, when feasible, an enclosed space for the verbal exchange of PHI.

**Exception:** In work environments structured with few offices or closed rooms, such as in some offices on the neighbor islands or any open office environment where uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur, such incidental uses or disclosures are not considered a violation provided that the DHS has met the reasonable Safeguards of this policy and the Minimum Necessary requirements DHS Privacy Policy No. 8.1.6, " Minimum Necessary Information".

c. Visual:

- i. DHS Staff must ensure that observable PHI is adequately shielded from unauthorized disclosure on computer screens and paper documents.
  - A. Computer screens: Each DHS workplace must make every effort to ensure that PHI on computer screens is not visible to unauthorized persons.
  - B. Paper documents: DHS Staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard PHI.

### 3. DHS administrative safeguards

- a. The DHS must:
  - i. Implement Role Based Access (RBA), which is a form of security allowing reasonable access to data based on job function, as discussed in the DHS Privacy Policy No. 8.1.6, "Minimum Necessary Information". DHS Staff must be assigned to an RBA group that may give members reasonable access only to the Minimum Necessary information to fulfill their job functions.
  - ii. Comply with the Minimum Necessary requirements of DHS Privacy Policy No. 8.1.6, "Minimum Necessary Information".
- b. DHS managers and supervisors must conduct reviews at least annually in order to evaluate and improve the effectiveness of their current safeguards.

<b>DHS</b>  <b>P&amp;PM</b>	<b>Subject</b> <b>Administrative, Technical and Physical</b> <b>Safeguards</b>	<b>Number</b> 8.1.8	<b>Page</b> 3 of 3
		<b>OPR</b> <b>Director's Office</b>	
		<b>Issue/Revision Date</b> April 14, 2003	

- c. DHS Staff must be provided training on the DHS Privacy Policies and Procedures, and the DHS must document that all DHS Staff has been provided this training.

#### 4.0 SCOPE


This policy applies to Covered Components of the DHS as listed in the Appendix B.

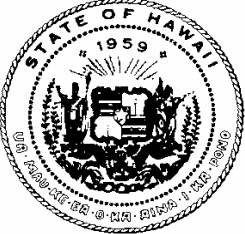
#### 5.0 RESPONSIBILITIES

Reserved for future use.

#### 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director

	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.1.9	Page 1 of 3
	Subject Enforcement, Sanctions, and Penalties for Violations of Client Privacy		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 1.0 PURPOSE

The intent of this policy is to specify Enforcement, Sanctions, and Penalties that may result from violation of the Department of Human Services (DHS) policies regarding the privacy and protection of Protected Health Information (PHI) and to offer guidelines on how to conform to those policies.

## 2.0 REFERENCES AND DEFINITIONS

### 2.1 REFERENCES

- a. 45 CFR 164.530

### 2.2 DEFINITIONS

See Glossary of Terms, Appendix A.

## 3.0 POLICY

### **1. General**

- a. DHS Staff must guard against improper uses or disclosures of PHI.
  - i. DHS Staff who are uncertain if a disclosure is permitted must consult with a supervisor or, if a supervisor is not available, the DHS Privacy Officer, prior to making the disclosure.
- b. Supervisors are responsible for assuring that DHS Staff who have access to PHI, whether it be electronic, hard copy, or oral, are informed of their responsibilities under the DHS Privacy Policies.
- c. DHS Staff who violate DHS policies and procedures regarding the safeguarding of PHI may be subject to disciplinary action.
- d. DHS Staff who knowingly and willfully violate State or Federal Law for improper use or disclosure of PHI may be subject to legal action, which includes but is not limited to criminal investigation and prosecution and/or civil monetary penalties.
- e. If the DHS fails to enforce privacy safeguards, the DHS as a State agency may be subject to administrative penalties by the Department of Health and Human Services (DHHS), including federal funding penalties.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Enforcement, Sanctions, and Penalties for Violations of Client Privacy	Number 8.1.9	Page 2 of 3
		Issue/Revision Date April 14, 2003	

## 2. Retaliation prohibited

- a. Neither the DHS as an entity nor any DHS Staff will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:
  - i. Any Client for exercising any right established under DHS Policy, or for participating in any process established under DHS Policy, including the filing of a complaint with the DHS or with the DHHS.
  - ii. Any Client or other person (including DHS Staff) for:
    - A. Filing a complaint with the DHS or with the DHHS as provided in General Privacy, DHS Privacy Policy No. 8.1.3, "Client Privacy Rights" section 3.7.b;
    - B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to the DHS Policies and Procedures.
    - C. Opposing any unlawful act or practice, provided that:
      - I. The Client or other person (including DHS Staff) has a good faith belief that the act or practice being opposed is unlawful; and
      - II. The manner of such opposition is reasonable and does not involve a use or disclosure of a Client's PHI in violation of DHS Privacy Policies.

## 3. Disclosures by whistleblowers

- a. A DHS Staff or Business Associate may disclose a Client's PHI if:
  - i. The DHS Staff or Business Associate believes, in good faith, that the DHS has engaged in conduct that is unlawful or that otherwise violates professional standards or DHS Policy, or that the care, services, or conditions provided by the DHS could endanger DHS staff, persons in DHS care, or the public; **and**
  - ii. The disclosure is to:
    - A. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the DHS;
    - B. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by the DHS; or,
    - C. An attorney retained by or on behalf of the DHS Staff or Business Associate for the purpose of determining the legal options of the DHS Staff or Business Associate with regard to this DHS Policy.

## 4. Mitigation of deleterious effect of a use or disclosure of PHI by DHS Staff

- a. The DHS must mitigate, to the extent practicable, any harmful effects of unauthorized uses or disclosures of PHI by DHS Staff.



<b>DHS</b>  <b>P&amp;PM</b>	Subject Enforcement, Sanctions, and Penalties for Violations of Client Privacy	Number 8.1.9	Page 3 of 3
		Issue/Revision Date April 14, 2003	

#### 4.0 SCOPE

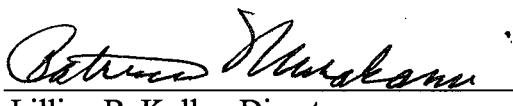
This policy applies to Covered Components of the DHS as listed in the Appendix B.

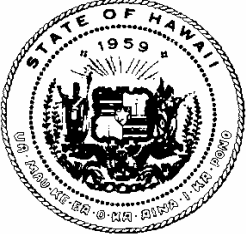
#### 5.0 RESPONSIBILITIES

Reserved for future use.

#### 6.0 DESCRIPTIVE PARAGRAPHS

Reserved for future use.

APPROVED:   
for Lillian B. Koller, Director

	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.3.A	Page 1 of 6
	Subject Appendix A Glossary of Terms		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 2.0 REFERENCES AND DEFINITIONS

### 2.1 REFERENCES

### 2.2 ACRONYMS

**CMS** - Centers for Medicare and Medicaid Services

**CLIA** - Clinical Laboratory Improvement Act

**DHS** - Hawaii Department of Human Services

**DHHS** – The U.S. Department of Health and Human Services

**HIPAA** - Health Insurance Portability and Accountability Act of 1996

**IIHI** -Individually Identifiable Health Information

**MOU** - Memorandum of Understanding aka Memorandum of Agreement

**OCR** - Office of Civil Rights

**PHI** - Protected Health Information

**RBA** - Role Based Access

**TPA** -Third Party Administrator

**TPO** - Treatment, Payment or Health Care Operations

### 2.3 DEFINITIONS

**Administrative Simplification:** The portion of HIPAA that gives the US Department of Health and Human Services (DHHS) the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers and employers; and to specify the types of measures required to protect the security and privacy of individually identifiable health care information.

**Business Associate:** A person or entity that receives PHI from a Covered Entity (such as the DHS) in order to perform a service for or on behalf of the Covered Entity, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management, and repricing. A Business Associate is also a person or entity that provides, other than in the capacity of a DHS employee, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the DHS, or for an organized health care arrangement in which DHS participates, where the provision of the service involves the disclosure of individually identifiable health information from the DHS, or from another business associate of the DHS, to the person or entity. A Business Associate may be a Covered Entity. The Business Associate definition excludes a person who is part of the DHS' workforce.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Appendix A Glossary of Terms	Number 8.3.A	Page 2 of 6
		Issue/Revision Date April 14, 2003	

**Centers for Medicare and Medicaid Services (CMS):** The federal agency that administers the Medicare and Medicaid programs. CMS has responsibility for implementing various provisions of HIPAA, including health insurance reform and administrative simplification.

**Client:** is an applicant, recipient or enrollee who requests or receives services from the Covered Components of the DHS.

**Clinical Laboratory Improvement Act (CLIA):** A federal law, which among other provisions, sets standards for performing clinical trials.

**Code Set:** Codes and their descriptors used to encode data elements, tables of terms, medical concepts, diagnostic codes or medical procedures.

**Correctional Institution:** Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witness, or others awaiting charges or trial.

**Covered Component (DHS):** A division, office or program of DHS designated by DHS as a health care component performing covered functions required to comply with the applicable requirements of the HIPAA Privacy and Security requirements and DHS Privacy and Security Policies.

**Covered Entity:** A health plan, health care clearinghouse, or health care provider that transmits information in electronic form in connection with a health care transaction.

**Data Element:** The smallest named unit of information in a transaction.

**Data Aggregation:** The combining of PHI to permit data analysis.

**Data Set:** A meaningful unit of information exchanged between two parties to a transaction.

**Data Use Agreement:** A written agreement to disclose a Limited Data Set between the DHS and another entity requiring that the entity receiving the Limited Data Set will use or disclose the Protected Health Information (PHI) only as specified in the written agreement with DHS.

**De-identified Information:** Client information from which DHS or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Appendix A Glossary of Terms	Number 8.3.A	Page 3 of 6
		Issue/Revision Date April 14, 2003	

**Department of Human Services (DHS):** In these policies, **the DHS** means DHS Covered Components.

**Department of Health and Human Services (DHHS):** The federal government department that has overall responsibility for implementing HIPAA.

**Designated Code Set:** A medical or administrative code set, which DHHS requires for use in one or more of the HIPAA standards.

**Designated Record Set:** Any collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for DHS Covered Components.

**DHS Privacy Officer:** A position designated by DHS to oversee all ongoing activities related to the development, maintenance, and adherence to department policies regarding the privacy of and accessibility to PHI, in accordance with State and Federal laws and best business practices. The DHS shall develop policies to indicate the Privacy Officer's duties and responsibilities.

**DHS Privacy Policies:** Department level requirements applicable to specified DHS divisions and offices (Covered Components) created to protect the privacy of individually identifiable health information in compliance with HIPAA requirements. These are the DHS HIPAA Privacy Policies contained in Section 8.1 of the DHS Policies and Procedures Manual.

**DHS Privacy Policies and Procedures:** Includes the DHS Privacy Policies and the respective division level policies and procedures developed for the protection of individually identifiable health information.

**DHS Staff:** In these policies, DHS Staff refers to the DHS workforce of DHS Covered Components, and includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DHS Covered Components, is under the direct control of the DHS, whether or not they are paid by the DHS.

**Disclosure:** The release, transfer or provision of; access to; or divulgence in any other manner of PHI to parties outside the entity holding the information.

**Disclosure History:** A list of any entities that have received individually identifiable health information, without written authorization, for uses unrelated to treatment and payment.

**Hawaii Uniform Practices Act:** Chapter 92F, Hawaii Revised Statutes, as amended.

**Health Care Clearinghouse:** A public or private entity that does either of the following: (1) processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; (2) receives a standard transaction from another entity and processes or

<b>DHS</b>  <b>P&amp;PM</b>	Subject Appendix A Glossary of Terms	Number 8.3.A	Page 4 of 6
		Issue/Revision Date April 14, 2003	

facilitates the processing of that information into a nonstandard format or nonstandard data content for a receiving entity.

**Health Care Provider:** A provider of medical or other health services or any other person or organization who furnishes, bills or is paid for health care in the normal course of business.

**Health Care Operations:** Under HIPAA, this is generally defined as conducting quality assessment and improvement activities; reviewing the competence or qualifications of health care professionals; capitation rate-setting, cost-sharing (including premium) determinations; conducting or arranging for medical review; legal services and auditing functions, including fraud and abuse detection and compliance programs; business planning; development management and general administrative activities as a function of the Health Plan.

**HIPAA - Health Insurance Portability and Accountability Act of 1996:** A federal law (Public Law 104-191) that focuses on protecting health insurance coverage for workers and their families when they change or lose their jobs (portability), and protecting health information and data integrity, confidentiality, and availability (accountability).

**Health Oversight:** Authorized by law to oversee the health care system (whether public or private), government programs in which health information is necessary to determine eligibility or compliance, or entities subject to government regulatory programs for which the information is necessary for determining compliance with program standards, or to enforce civil rights laws for which health information is relevant.

**Hybrid Entity:** A covered entity whose business activities or components include both covered (perform activities that include the creation, receipt, maintenance and transmission of PHI) and non-covered functions (do not perform activities that include the creation, receipt, maintenance and transmission of PHI).

**Individually Identifiable Health Information (IIHI):** Information that is a subset of health information, including demographic information collected from an individual, which (1) identifies the individual, or (2) could be used to identify the individual.

**Inmate:** An individual in lawful physical custody of a correctional institution. An individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody. *Persons held in lawful custody* includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

**Knowing and Willful Violation:** A violation of DHS Privacy Policies committed in which the individual committing the violation was in possession of the knowledge or understanding that their action(s) were in violation of DHS Privacy Policies; and, the violation was committed deliberately by that individual.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Appendix A Glossary of Terms	Number 8.3.A	Page 5 of 6
		Issue/Revision Date April 14, 2003	

**Legal Representative:** means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in *loco parentis* who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting in *loco parentis* has assented to an agreement of confidentiality between the provider and the minor.

**Limited Data Set:** PHI that excludes certain direct identifiers of the individual, or of relatives, employers or household members of the individual.

**Memorandum of Understanding/Agreement (MOU):** An agreement between governmental entities who share PHI established to meet requirements of the DHS Privacy Policies with regard to the protection of PHI.

**Minimum Necessary:** When using or disclosing PHI (or requesting PHI from another covered entity), a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

**Office of Civil Rights (OCR):** The office within DHHS with primary responsibility for implementation and monitoring of HIPAA privacy requirements.

**Protected Health Information (PHI):** “Protected Health Information” which is individually identifiable health information (except certain educational records and employment records), including health and demographic information about an individual that is transmitted or maintained in any medium where the information:

- Is created or received by a health care provider, health plan, employer or health care clearinghouse; and
- Relates to the past, present or future physical or mental health condition of an individual, provision of health care to an individual, or payment for the provision of health care to an individual;
- Identifies the individual; or
- With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

**Psychotherapy Notes:** Notes recorded (in any medium) by a mental health professional documenting or analyzing contents of conversations that took place during any form of counseling session that are separate from the individual’s medical record. This does not include prescriptions and monitoring, counseling session start and end times, frequency of treatment, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date.

<b>DHS</b>  <b>P&amp;PM</b>	Subject Appendix A Glossary of Terms	Number 8.3.A	Page 6 of 6
		Issue/Revision Date April 14, 2003	

**Public Official:** An employee of a government agency who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency.

**Reasonable Safeguard:** Covered entities must make reasonable efforts to prevent uses and disclosures not permitted by this Manual.

**Research:** A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

**Risk Mitigation:** Actions taken to reduce the likelihood of a risk occurring as a problem, or to reduce the impact if it does occur.

**Role Based Access (RBA):** A form of security that allows access to electronic data/information based on job function and the DHS security procedures.

**Routine and Recurring:** The disclosure of PHI to government agencies, DHS components or other persons or entities as required by law, as required for legal services or as necessary for health care operations without the authorization of the individual, for a purpose that is compatible with the purpose for which the information was collected.

**State and/or Federal Law:** State and/or Federal government statutes, administrative code, rules or regulations.

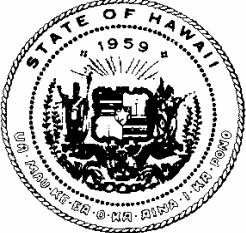
**Third Party Administrator (TPA):** An entity that processes health care claims and performs related business functions for a health plan.

**Treatment, Payment or Health Care Operations (TPO):** Covered functions of the health plan for which authorization is not required for the sharing of PHI and includes all of the following:

- Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
- Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collection activities, medical necessity determinations and utilization review.
- Operations *see Health Care Operations above.*

**Transaction:** The exchange of information between two parties to carry out financial or administrative activities related to health care.

**Use:** The sharing, employment, application, utilization, examination or analysis of PHI within the entity that maintains such information.

	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.3.B	Page 1 of 1
	Subject Appendix B Declaration of Hybrid Entity Status and list of Covered Components		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

### **The DHS Declaration of Covered Entity Status**

The Department of Human Services (DHS) is a Hybrid Entity. The following components of the DHS have been designated as Covered Components:

The Director's Office

The Med-QUEST Division

The following components of the Social Services Division (SSD):

Social Services Division Administration

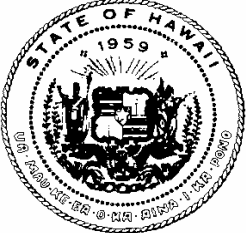
Support Services Office Administration

Medicaid Waiver Staff

Adult and Community Care Services Branch: Medicaid Waiver Programs

Effective 4/14/03.



	<b>Department of Human Services POLICIES AND PROCEDURES MANUAL</b>		Number 8.3.C	Page 1 of 2
	Subject Appendix C DHS HIPAA Related Forms		OPR Director's Office	
			Issue/Revision Date April 14, 2003	

## 8.0 DHS HIPAA RELATED FORMS

### A. Med-QUEST Division

1. **(8030) Notice of Privacy Practices**
2. **(1123) Authorization to Disclose Confidential Information by the Med-QUEST Division**
3. **(1124) Authorization to Disclose Confidential Information to the Med-QUEST Division**
4. **(8020) Notice of Authorization/Acknowledgement**
5. **(8021) Determination of DHS 1123 (internal for MQD use only)**
6. **(8022) Notice of Denial to Disclose Confidential Information (to client)**
7. **(8023) Request for Confidential Information (notice of determination to third party)**
8. **(8024) Request to Amend Confidential Information**
9. **(8025) Request to Amend Confidential Information (Notice of Determination)**
10. **(8026) Request to Amend Confidential Information (Notice of Rebuttal)**
11. **(8027) Request for Accounting of Disclosures of Health Information**
12. **(8028) Request to Restrict Disclosure of Protected Health Information**

### B. Social Services Division

1. **(1681) Notice of Privacy Practices**
2. **(1557) Authorization to Disclose Confidential Information to the Department of Human Services**
3. **(1558) Authorization to Disclose Confidential Information by the Department of Human Services**

<b>DHS</b>  <b>P&amp;PM</b>	Subject Appendix C DHS Required Forms	Number 8.3.C	Page 2 of 2
		Issue/Revision Date April 14, 2003	

4. **(1689) Determination of DHS 1558 (Notice of Denial to Disclose Confidential Information)**
5. **(1690) Notice of Denial to Disclose Confidential Information**
6. **(1691) Response to Request to Release Non-Routine Protected Health Information**
7. **(1692) Request to Amend Confidential Information**
8. **(1693) Request to Amend Confidential Information (Notice of Amendment Determination)**
9. **(1694) Request to Amend Confidential Information (Notice of Rebuttal)**
10. **(1695) Request for Accounting of Disclosures of Protected Health Information (Notice of Availability)**
11. **(1696) Request to Restrict Disclosures of Protected Health Information**
12. **(1697) Privacy Program Statement of Understanding**
13. **(1698) Client's Declaration of Custody of the Client Information Notebook**
14. **(1699) Response to Client – Request for Access to Confidential Information**